Best Practices Guide

McAfee® ePolicy Orchestrator® 4.0 and 4.5

COPYRIGHT
Copyright © 2011 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS
AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1 Preface **7**

About this guide 7
Audience 7
Conventions 7
What's in this guide 7
Finding product documentation 8

1 History of McAfee ePolicy Orchestrator software **9**

2 ePolicy Orchestrator product architecture **11**

Architecture overview 11
Hardware configuration 13
Configuration of McAfee ePO server and SQL Server on the same physical server 13
Use VMs for the McAfee ePO Server 14
Share the SQL database hardware 14
Hard disk configuration 14
SAN usage 17
Determining the server hardware needed 17

3 Repositories **21**

Repositories overview 21
FTP repositories 22
HTTP repositories 22
UNC share repositories 22
SuperAgent repositories 23
Creating a new SuperAgent policy 24
Creating a new group in the System Tree 24
Assigning the new SuperAgents policy to the new SuperAgents group 25
Dragging a system into the new SuperAgents group 26
Place repositories 27
Calculating bandwidth of repository replication 28
Calculating bandwidth for client pulls of updates 28
Determine repository count 29
Global updates 32

4 Agent Handlers **35**

Agent Handlers overview 35

5 Installation and upgrade of ePolicy Orchestrator software **37**

Install new software 37
Upgrade the software 37
Move the server 39
Move McAfee Agents between servers 40
Using Transfer Systems 41

6 McAfee Agent 43
Agent functionality . . . 43
Deploying agents . . . 44
Deploy from the McAfee ePO server . . . 46
Synchronize with Active Directory . . . 46
Deploy the agent using third-party tools . . . 47
Make the agent part of your image . . . 48

7 Organizing your System Tree 51
Your System Tree . . . 51
Use Active Directory synchronization . . . 51
Dynamically sorting your machines . . . 52

8 Policies and packages 55
Manage policies . . . 55
McAfee agent policy . . . 56
Agent to server communication interval (ASCI) . . . 56
Configuring the policy enforcement interval . . . 59
Deploying packages . . . 60

9 Client tasks 63
Deploy products . . . 63
Configuring which products are deployed . . . 64
Schedule product deployment with randomization . . . 64
Updating products . . . 65

10 Server tasks 69
Perform an action on a query . . . 69
Creating a server task . . . 70
Creating an automatic report email or export . . . 71
Create an automatic content pull and replication . . . 72
Disabling master repository client pulls . . . 73
Purge events automatically . . . 74
Creating a purge events by query server task . . . 74
Purging events by query . . . 76
Deleting inactive systems automatically . . . 77

11 Reporting 81
Reporting overview . . . 81
Custom queries . . . 82
Creating custom event queries . . . 84
Event summary queries . . . 88
Creating custom table queries . . . 95

12 FAQ and common scenarios 99
Determining if you have a duplicate GUID problem . . . 99
Determining if your server has performance problems . . . 100
Understand product version numbers . . . 102
Determining the best upgrade strategy . . . 103
1051 and 1059 events . . . 103
Filtering 1051 and 1059 events . . . 104

13 SQL maintenance 105
ePolicy Orchestrator SQL database maintenance . . . 105

14 Disaster recovery **107**
Configuring simple disaster recovery 107
Use server clusters for disaster recovery 108
Use cold and hot spares on one physical site 108
Use cold and hot spares on two physical sites 108

15 Reference documentation **111**

Index **113**

Preface

Contents

- *About this guide*
- *Finding product documentation*

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input` or `Path`	Commands and other text that the user types; the path of a folder or program.
`Code`	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

What's in this guide

Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a **Product**, then select a **Version**. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 History of McAfee ePolicy Orchestrator software

ePolicy Orchestrator software is a mature security management platform that delivers the quality and stability that can only be provided by a product that has evolved in the security environment.

Understanding the history of the ePolicy Orchestrator software and the initial products it managed can help you use the information in this Best Practices Guide more effectively.

ePolicy Orchestrator software was originally released in 1999 when computer security was just beginning as an industry. McAfee had already released one of its first anti-virus client products and it was being deployed worldwide using floppy disks exchanged by users. Soon users asked, "how do I manage it once I have it deployed?"

At first the only management tool offered was called Management Edition 1.0 which had several limitations. McAfee rewrote the management server product and the ePolicy Orchestrator software 1.0 was born. Today, it has evolved to manage:

- McAfee VirusScan Enterprise — Used with Microsoft Windows, Macintosh, and Linux versions
- McAfee Host Intrusion Prevention and Windows Firewall — Provides multiple operating system support
- McAfee SiteAdvisor — Provides URL reputation filtering on the endpoint
- McAfee Policy Auditor — Provides comprehensive systems auditing on multiple operating system's
- McAfee Network Access Control — Controls access to network resources based on policy
- McAfee Application Control — Prevents unauthorized programs from running
- McAfee Endpoint Encryption — Provides full disk encryption to prevent data loss systems
- McAfee Data Loss Protection — Controls USB devices and unauthorized removal of data
- McAfee Encrypted USB Drives — Manages USB drives with hardware encryption

This list does not include the numerous integrations with McAfee Security Innovation Alliance (SIA) Partners and integration with McAfee Network products. Some of these McAfee integrated products include Web Gateway, Network Intrusion Prevention, and Vulnerability Manager.

2 ePolicy Orchestrator product architecture

The ePolicy Orchestrator software architecture offers extensive functionality that can be configured many different ways. It uses a classic client-to-server model where the client calls the McAfee ePO server asking for instructions.

Contents

- *Architecture overview*
- *Hardware configuration*
- *Hard disk configuration*
- *SAN usage*
- *Determining the server hardware needed*

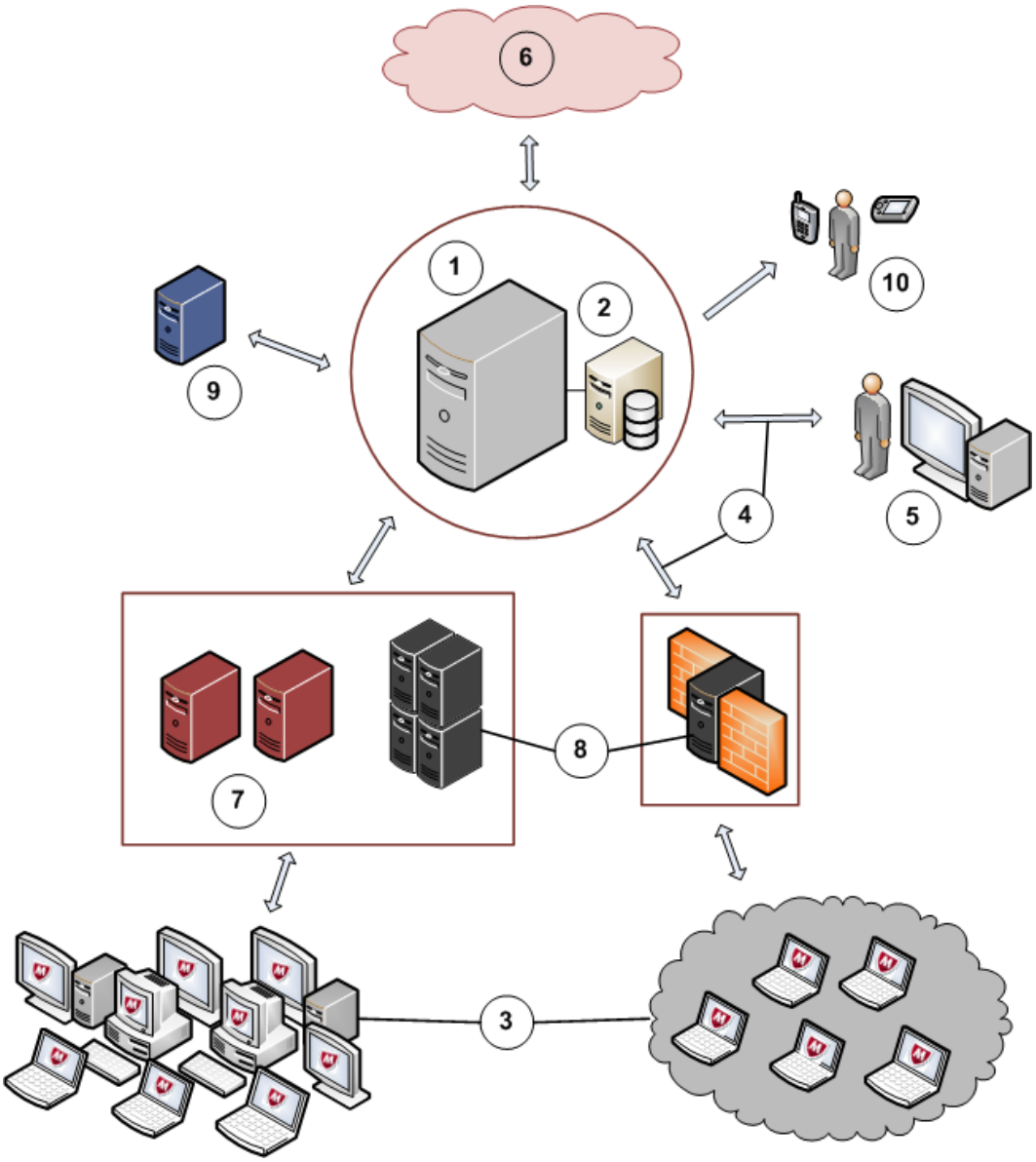
Architecture overview

The architecture of the ePolicy Orchestrator software and its components provides all of the functionality needed to manage and protect your environment.

The ePolicy Orchestrator server provides these major functions:

- Manages and deploys product policies
- Enforces those policies on all your endpoints
- Distributes all the McAfee software including new products, upgrades, patches, and new content
- Reports on the enterprise network using many predefined reports or customized reports you create

The following figure shows the major ePolicy Orchestrator components.



1 **ePO server** — Connects to the McAfee update server to download the latest security content

2 **ePO Microsoft SQL database** — Stores all the data about the managed systems on your network

3 **McAfee Agents** — Provides policy enforcement, product deployments and updates, and reporting on your managed systems

4 **Agent-server secure communication (ASSC) connections** — Provides communications that occur at regular intervals between your systems and server

> If remote Agent Handlers are installed in your network, agents communicate with the server through their assigned Agent Handlers.

5 **Web console** — Allows users to log on to the ePolicy Orchestrator console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies

6 **McAfee update server** — Hosts the latest security content so your ePolicy Orchestrator can pull the content at scheduled intervals.

7 **Distributed repositories** — Installed throughout your network to host your security content locally, so agents can receive updates more quickly

8 **Remote Agent Handlers** — Helps to scale your network to handle more agents with a single ePolicy Orchestrator server

9 **Ticketing system** — Connects to your ePolicy Orchestrator server to help manage your issues and tickets

10 **Automatic responses** — Provides notifications sent to security administrators when an event occurs

Hardware configuration

The physical hardware configuration you use for the McAfee ePO server and SQL Server is determined primarily by the number of nodes, or node count, these servers manage.

Previous versions of McAfee ePolicy Orchestrator could easily manage up to 200,000 nodes using one ePolicy Orchestrator server with a separate SQL Server. But the latest versions of McAfee ePolicy Orchestrator have many more features and are much more robust changing the number of nodes it can manage efficiently. Now McAfee ePolicy Orchestrator can manage up to 50,000 nodes with basic server hardware and reasonable planning. Once you pass 50,000 nodes it becomes much more important how you configure your McAfee ePO server hardware for the best possible performance.

Initially your managed node count determines your ePolicy Orchestrator server platform and the recommended hardware specifications. The node count helps you answer these questions:

- Can I install the McAfee ePO server and SQL Server on the same physical hardware?
- Can I use a virtual machine for McAfee ePolicy Orchestrator or the SQL Servers?
- Can McAfee ePolicy Orchestrator use an existing SQL Server running other databases for McAfee ePolicy Orchestrator?
- How do I partition my hard disk drives for the McAfee ePO server and SQL Server?

Configuration of McAfee ePO server and SQL Server on the same physical server

You must determine the number of nodes you want the McAfee ePO server and SQL Server to manage before you know if both servers can be installed on the same physical server.

Environments up to 5,000 or 10,000 nodes can have the McAfee ePO server and SQL Server installed on one physical server to save hardware, IT, and energy costs. This works if you:

- Optimize your storage using multiple dedicated drives (see *Hard disk configuration*) for each application as your node count increases
- Manage only the basic McAfee products, such as VirusScan Enterprise and Host Intrusion Prevention

If in the future if you plan to manage more McAfee products and to add many more nodes, split the one server into two physical servers, one dedicated to the McAfee ePO server and the other for the SQL Server.

Use VMs for the McAfee ePO Server

The McAfee ePO server supports multiple versions of virtual environments, but when your node count reaches 25,000 to 30,000 nodes you run into the most common virtual machine (VM) bottleneck, disk performance.

To install the McAfee ePO server on a VM and solve this disk performance problem, you must:

- Dedicate physical disks to the McAfee ePO server in the VM.
- Assign priority for the CPUs to the McAfee ePO server.

You can also use a SQL Server database installed on a VM for the McAfee ePO server, but not if your node count exceeds 25,000 to 30,000 nodes, because of the same disk performance bottleneck.

Share the SQL database hardware

You can install the McAfee ePO server SQL database on a shared SQL Server.

However, it is important to remember that the McAfee ePO server SQL database performs thousands of disk reads and writes every few seconds, which can negatively impact performance on an over utilized SQL Server.

You can share your existing fully clustered, redundant and centrally managed SQL environment if:

- The shared SQL Server is not already over utilized.
- Your McAfee ePO server managed node count is less than 20,000.
- Other SQL database functions do not cause spikes that could slow the McAfee ePO server SQL database reads and writes.

Node count	ePO and SQL on one server	Use VM server	ePO DB on shared SQL Server
100-5,000	OK	Optional	Optional
5,000-25,000	Optional	Optional	Optional
25,000-75,000	Not recommended	Not recommended	Not recommended
75,000 or more	No	No	No

Hard disk configuration

When it comes to configuring your McAfee ePO server hardware, the hard disk configuration is one of the most important factors for larger ePO environments.

Your McAfee ePO server processes thousands of events from multiple products, which must be written to the SQL database. Plus, when you use the McAfee ePO server to administer your network and to execute queries, ePolicy Orchestrator software accesses the SQL Server database for millions of events and thousands of nodes. These functions make disk configuration one of the most important factors for larger McAfee ePO server implementations.

The primary limiting factor when choosing your configuration is the cost of storage. Depending on your hardware budget, choose the best configuration to prepare for future growth even though now you might only have 5,000 nodes to manage with the McAfee ePO server. If your budget allows, choose the best and fastest configuration that you can afford.

Manage fewer than 5,000 nodes

If you have fewer than 5,000 nodes to manage with the McAfee ePO server, disk configuration is rarely an issue. Use your normal procedure for configuring the disks on the server. Typically assign individual disks to the:

- Operating system
- McAfee ePolicy Orchestrator
- SQL database

If you are using RAID for redundancy then any form of RAID is adequate and most organizations use RAID 5 as a standard. The following example shows this typical disk configuration.

Disk partition and RAID configuration for fewer than 5,000 nodes

Manage 5,000 to 25,000 nodes

If you have 5,000 to 25,000 nodes to manage with the McAfee ePO server, and you use one physical server for the McAfee ePO server and the SQL Server, then you must provide a physical disk for the:

- Operating system
- McAfee ePolicy Orchestrator
- SQL database

McAfee recommends you use RAID 1 and RAID 10 for this configuration instead of the standard RAID 5, especially if you use one physical server for both the McAfee ePO server and the SQL Server. The following example shows this RAID disk configuration.

Disk partition and RAID configuration for 5,000 to 25,000 nodes

Manage 25,000 to 75,000 nodes

If you have 25,000 to 75,000 nodes to manage with the McAfee ePO server, use two separate servers. For the McAfee ePO server, use:

- RAID 1 for the operating system
- RAID 10 for the ePO application

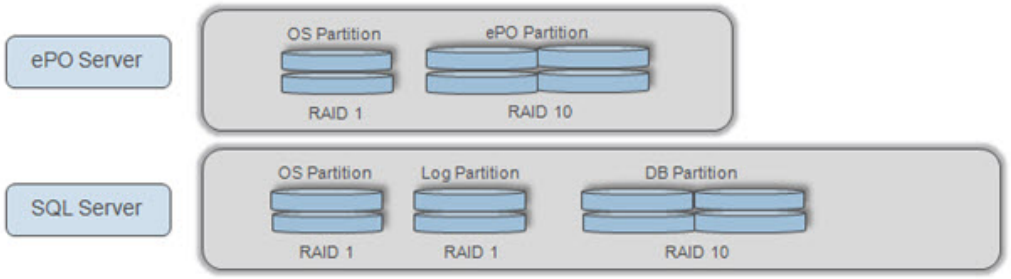
For the SQL Server, use:

- RAID 1 for the operating system with individual partitions for the SQL database (the MDF file) and the SQL transaction log (the LDF file).
- RAID 1 for the log partition
- RAID 10 for the database partition

To manage this size organization with the McAfee ePO server, McAfee recommends you use RAID 10 for the SQL Server.

The following example shows this RAID disk configuration.

Disk partition and RAID configuration for 25,000 to 75,000 nodes



Manage more than 75,000 nodes

If you have more than 75,000 nodes to manage with the McAfee ePO server, use two separate servers. For the McAfee ePO server, use:

- RAID 1 for the operating system
- RAID 10 for the ePO application

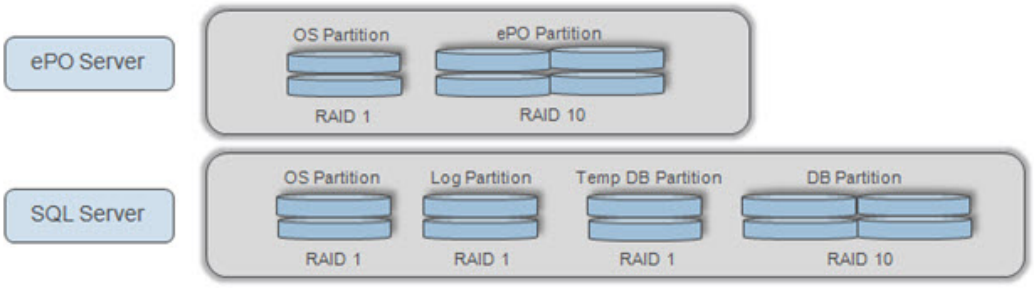
For the SQL Server, use:

- RAID 1 for the operating system, and provide individual partitions for the SQL database (the MDF file), the SQL transaction log (the LDF file), and the SQL Temp database
- RAID 10 for the database partition

To manage this size organization with the McAfee ePO server, McAfee recommends you use RAID 10 for the SQL Server.

The following example shows this RAID disk configuration.

Disk partition and RAID configuration for more than 75,000 nodes



SAN usage

Storage area network (SAN) devices are the standard configuration for larger storage requirements such as SQL databases that require backup and maintenance. SAN storage is a valid method for storing your SQL database, but adds a potential layer of complexity to your SQL implementation that should be understood.

A SAN engineer might maintain the SAN and not be familiar with McAfee ePolicy Orchestrator and its heavy I/O requirements. If you deploy the McAfee ePO server SQL database on a SAN you must have your SAN engineer involved early in the process to assist in planning your architecture.

Many SANs are grouped into a generic classification known as *tiers*. The three tiers are:

- Tier 1 SAN — The most expensive, fastest, and redundant storage array. If you have 75,000 nodes or more, use a tier 1 SAN to store your SQL database.
- Tier 2 SAN — Used to store critical data that requires redundancy. Plus, this data is accessed often but does not perform excessive transactions on the SAN.
- Tier 3 SAN — Used for databases that do not require much space and have little I/O.

Refer to the following articles that describe putting the SQL database on a SAN:

- Deploying SQL Server 2005 with SAN #1
- Deploying SQL Server 2005 with SAN #2
- Deploying SQL Server 2005 with SAN #3

Determining the server hardware needed

The critical questions to ask are, how many McAfee ePO servers and SQL Servers do I need and what hardware should I use? Remember, the primary job of the McAfee ePO server is to distribute policies and collect events.

The McAfee ePO server does not have to distribute any McAfee software or content. You might think you need one McAfee ePO server for each major geographical region for efficient bandwidth utilization, but that is not true. Many McAfee ePO server users with large and small offices dispersed all over the world use only one McAfee ePO server. These users have repositories, which are simple file shares, at each office to handle the distribution of content. See *Repositories*.

There is no technical limit on how many nodes can be managed by one McAfee ePO server. The key concept to remember about McAfee ePO servers is *less is better*. The fewer McAfee ePO servers you have the easier it is to maintain your environment. There are many McAfee ePO server users with 200,000 nodes being managed by one server.

The theoretical limit of McAfee ePO servers in relationship to managed nodes is even higher with the new Agent Handler technology added to the ePolicy Orchestrator software version 4.5.

When choosing the operating systems for your servers, use 64-bit versions, where applicable, for improved performance. This means the operating system for both the SQL Server application and SQL database requires 64-bit versions where possible, if the hardware supports it.

The following sections offer hypothetical environments to provide some guidelines for organization size and hardware requirements.

These example provide minimum requirements for hardware. McAfee recommends you exceed these requirements to improve performance and allow for growth, wherever possible.

The McAfee ePO server performance is determined by the SQL database, where the McAfee ePO server data is stored. It is the main workhorse behind the McAfee ePO server application. The three items that affect SQL performance are CPU, RAM, and disk performance. These three items control the responsiveness of the McAfee ePO server application, from a SQL perspective. McAfee recommends you exceed the minimum recommendations wherever possible.

The following table lists the hardware recommend for the various organization sizes.

Organization size	Node count	McAfee ePO server			SQL Server		
		CPU processors	RAM	Hard drive	CPU processors	RAM	Hard drive
Small	100 – 5,000	2	4 GB	20 GB	N/A	N/A	N/A
Medium	5,000 – 25,000	2	4 – 8 GB	20 – 40 GB	4	8 – 16 GB	100 GB
Large	25,000 – 75,000	4	8 –16 GB	20 – 40 GB	8	16 – 32 GB	150 GB
Very large	75,000 – 150,000	8	16 – 32 GB	40 – 80 GB	16	32 – 128 GB	300 GB

Small organization example

A small organization ranges from 100 to 5,000 nodes. You can reduce hardware costs by installing the McAfee ePO server and SQL database on the same physical server for a small organization. This small organization is easily managed by the McAfee ePO server and offers room for growth. You can also have multiple McAfee products deployed in the environment like VirusScan Enterprise, Host Intrusion Prevention, and Endpoint Encryption.

The hardware used for McAfee ePO server and SQL database must be up-to-date hardware with these minimum requirements:

- Dual processor CPU
- 4 GB of RAM
- 20 GB of free hard drive space

The ePolicy Orchestrator software 4.5 installation is bundled with Microsoft SQL Express for installing McAfee ePO server in very small environments. Microsoft does not allow the SQL Express database to exceed 4 GB. The SQL Express database can only be used for testing the McAfee products and can also be used in production environments with fewer than 500 nodes.

Medium organization example

A medium organization ranges from 5,000 to 25,000 nodes. A single McAfee ePO server can easily manage this size organization with properly placed repositories to update content and software to the agents.

As your node count approached 25,000 nodes, McAfee recommends that you separate the McAfee ePO server and SQL Servers on their own physical servers. If hardware is limited, the McAfee ePO server and SQL Servers can reside on the same physical server, but McAfee recommends that you increase the hardware size as much as possible.

The minimum McAfee ePO server and SQL hardware recommended to manage this medium size organization is:

- Quad processor CPU
- 8 – 16 GB of RAM
- 100 GB of hard drive space if ePO and SQL database reside on the same hardware

Large organization example

A large organization ranges from 25,000 to 75,000 nodes. A single McAfee ePO server can manage the reporting of all McAfee products in the environment with properly placed repositories to update content and software to the agents. In a large organization, the McAfee ePO server and SQL Server must reside on separate physical hardware due to the amount of processing that occurs on the SQL database.

The minimum McAfee ePO server hardware recommended to manage this large size organization is:

- Quad processor CPU
- 8 – 16 GB of RAM
- Disk space is not a concern since all the data is stored in the SQL database

The minimum SQL Server hardware recommended to manage this large size organization is:

- 4 or 8 processors
- 16 to 32 GB of RAM
- At least 150 GB of space for the SQL database

For example, as you approach managing 75,000 nodes, use the highest performance server hardware. Your SQL Server needs 8 processors and 32 GB of RAM.

Very large organization example

A very large organization ranges from 75,000 to 150,000 nodes. This size organization is reaching the limits of the McAfee ePO SQL Server, use the highest performance hardware you can afford.

The minimum McAfee ePO server hardware recommended to manage this very large organization is:

- 8 processors
- 16 – 32 GB of RAM
- Disk space is not a concern since all the data is stored in the SQL database

The minimum SQL Server hardware recommended to manage this very large organization is:

- 16 processors
- 32 – 128 GB of RAM
- At least 300 GB of space for the SQL database

These are not upper limits for hardware. If you have the budget for additional hardware resources, exceed these recommendations.

3 Repositories

A repository is a file sharing device that serves out files for clients to download. It does not manage policies, collect events, or have any code installed. Policies and events are always handled by the McAfee ePO server or Agent Handler.

Contents

- *Repositories overview*
- *FTP repositories*
- *HTTP repositories*
- *UNC share repositories*
- *SuperAgent repositories*
- *Place repositories*
- *Calculating bandwidth of repository replication*
- *Calculating bandwidth for client pulls of updates*
- *Determine repository count*
- *Global updates*

Repositories overview

Repositories allow agents to pull software they need based on the client tasks you create in the McAfee ePO server.

Repository downloads include:

- Software
- Content
- Signatures or DAT files
- Patches

The McAfee ePO server always acts as the master repository. It keeps the master copy of all the content needed by your agents. The McAfee ePO server replicates that content to your distributed repositories. This allows your agents an alternate and closer source to use for their updates.

The McAfee ePO server requires no configuration to make it the master repository. It is the master repository by default.

Repository types include:

- FTP repositories
- HTTP repositories

- UNC share repositories
- SuperAgents

There are several things to keep in mind about these repositories:

- The McAfee ePO server requires certain protocols be used for the repositories, but any server vendor can provide those protocols. For example, if you use an HTTP repository you can use either Microsoft Internet Information Services (IIS) or Apache server (Apache is the faster option).
- The McAfee ePO server has no requirement for what operating system the repository uses. As long as the McAfee ePO server can access the folders you specify to copy its content to and as long as the agents can connect to the folder to download their updates everything works as expected
- Your agent updates and ePO replication are only as good as your repositories. If you are already using one of these repositories and your environment works well, then do not change the configuration.

If you are starting with a new installation, with no repositories, use a SuperAgent because they are easy to configure and reliable.

FTP repositories

You can use an FTP server to host a distributed McAfee ePO server repository. You might already have FTP servers in your environment and you can allow McAfee content to reside there as well.

FTP repositories are:

- Generally fast
- Can manage extensive load from the clients pulling data
- Helpful in a DMZ where HTTP may not be optimal and UNC shares can't be used

Using FTP servers your clients do not need authentication and can use anonymous logon to pull their content. No authentication reduces the chance a client might fail to pull its content.

HTTP repositories

You can use an HTTP server to host a distributed McAfee ePO server repository. You might already have HTTP servers in your environment placed in the proper regional locations.

HTTP servers can be very fast serving out files to large environments. An HTTP server like Apache is a good example. Your HTTP servers allow clients to pull their content without authentication. No authentication reduces the chance a client might fail to pull its content.

UNC share repositories

You can use Universal Naming Convention (UNC) shares to host your McAfee ePO server repository. Since most administrators are familiar with the concept of UNC shares this might seem like the easiest method to choose. But, this might not be true.

If you chose to use UNC shares, you must:

1. Create the folder
2. Adjust share permissions
3. Change the NTFS permissions
4. Create two accounts, one with read and another with write access

All of these tasks increase the chance of failure since these processes must be completed manually risking human errors. Your agents might not properly update if your agents cannot authenticate to your UNC share because they are not part of the domain or the credentials are incorrect

SuperAgent repositories

A SuperAgent is a way of creating a McAfee ePolicy Orchestrator repository. The advantage of a SuperAgent is that it is created with the McAfee ePO server and the McAfee Agent.

Using a McAfee SuperAgent reduces the chance of error because you don't rely on other protocols. Also, the process is less prone to human error because there is minimal data entry, no shares to create beforehand, and no user permissions to adjust. A SuperAgent simply uses any existing McAfee Agent in your environment and does not require any additional software other than the agent itself. For example, if you have 20,000 McAfee Agents you can easily choose a few to designate as SuperAgents via policy.

SuperAgents have these advantages:

- Any machine running a McAfee Agent can be designated as a SuperAgent just by changing its policy.
- You don't have to connect to the machine to create any shares, set up permissions, or rely on any Microsoft technology such as UNC shares.
- You don't have to open ports to enable the SuperAgent functionality. The SuperAgent needs only one open port, the agent wake-up call port you already defined for all your agents (8081 is the default port).
- You don't have to replicate credentials to SuperAgents. Since your McAfee ePO server is instantly aware of your SuperAgents, it manages replication and adjusts which SuperAgent your clients choose to use for their downloads.

To create a SuperAgent requires these four general tasks. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for detailed configuration steps.

1. Create a new SuperAgents policy.
2. Create a new group in the System Tree, for example named *SuperAgents.*
3. Assign the new SuperAgents policy to the new *SuperAgents* group.
4. Drag a system into the new "SuperAgents" group.

Once you have created the new "SuperAgents" group you can drag any system into that group and it become a SuperAgents the next time it communicates with the McAfee ePO server.

The following sections describe this process.

Creating a new SuperAgent policy

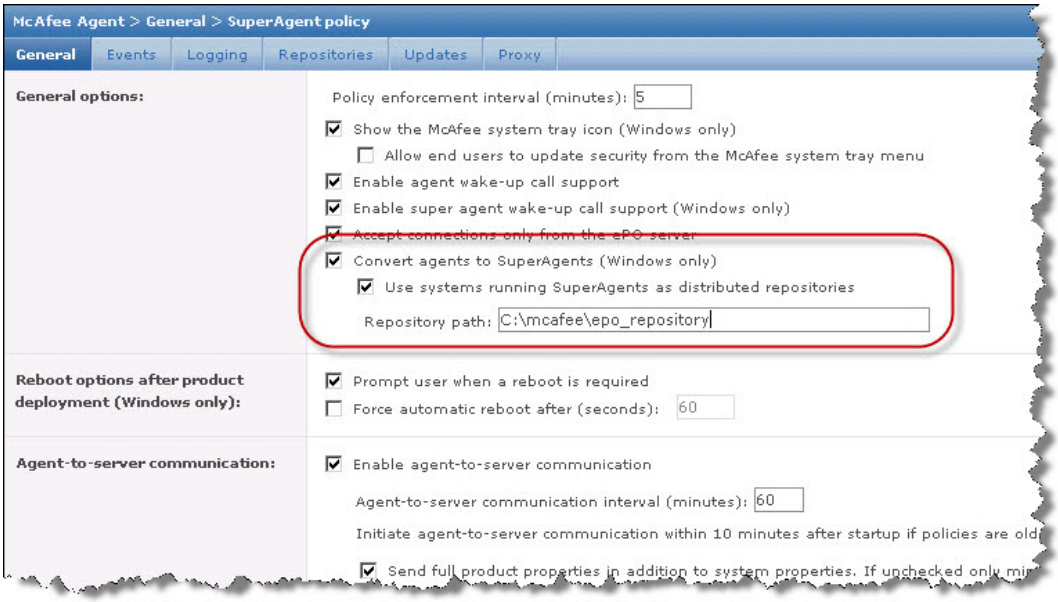
A SuperAgent policy allows you to assign that policy to client machines to convert them to SuperAgents.

Task

1 From the Policy Catalog, click **McAfee Agent** and from the Category list, select **General** to create a new policy.

> Give the new policy a distinctive name, for example `SuperAgent policy`. A common mistake is accidentally changing your primary McAfee Agent policy and turning all your nodes into SuperAgents.

2 From the General tab, click **Convert agents to SuperAgents** and **Use systems running SuperAgents as distributed repositories**, then type a folder path location for the repository.


McAfee Agent > General > SuperAgent policy
General
Events
Logging
Repositories
Updates
Proxy
General options:
Policy enforcement interval (minutes): 5
Show the McAfee system tray icon (Windows only)
Allow end users to update security from the McAfee system tray menu
Enable agent wake-up call support
Enable super agent wake-up call support (Windows only)
Accept connections only from the ePO server
Convert agents to SuperAgents (Windows only)
Use systems running SuperAgents as distributed repositories
Repository path: C:\mcafee\epo_repository
Reboot options after product deployment (Windows only):
Prompt user when a reboot is required
Force automatic reboot after (seconds): 60
Agent-to-server communication:
Enable agent-to-server communication
Agent-to-server communication interval (minutes): 60
Initiate agent-to-server communication within 10 minutes after startup if policies are old
Send full product properties in addition to system properties. If unchecked only mi

3 **Save** the new policy.

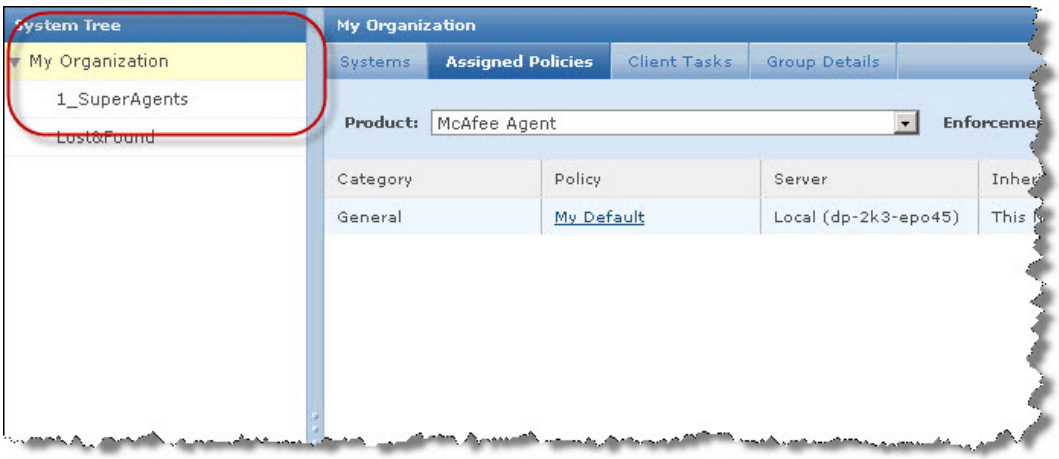
Creating a new group in the System Tree

With a SuperAgent group in your System Tree you can assign the SuperAgent policy to the group.

Create a new group in the System Tree called *1_SuperAgents*.

Task

1 From the System Tree, click **System Tree Actions** | **New Subgroup** and give it a distinctive name, for example *1_SuperAgents*.



2 Click **OK**. The new group appears in the System Tree list.

Assigning the new SuperAgents policy to the new SuperAgents group

When you assign the SuperAgents policy to the new SuperAgents group you complete the configuration of the SuperAgent group.

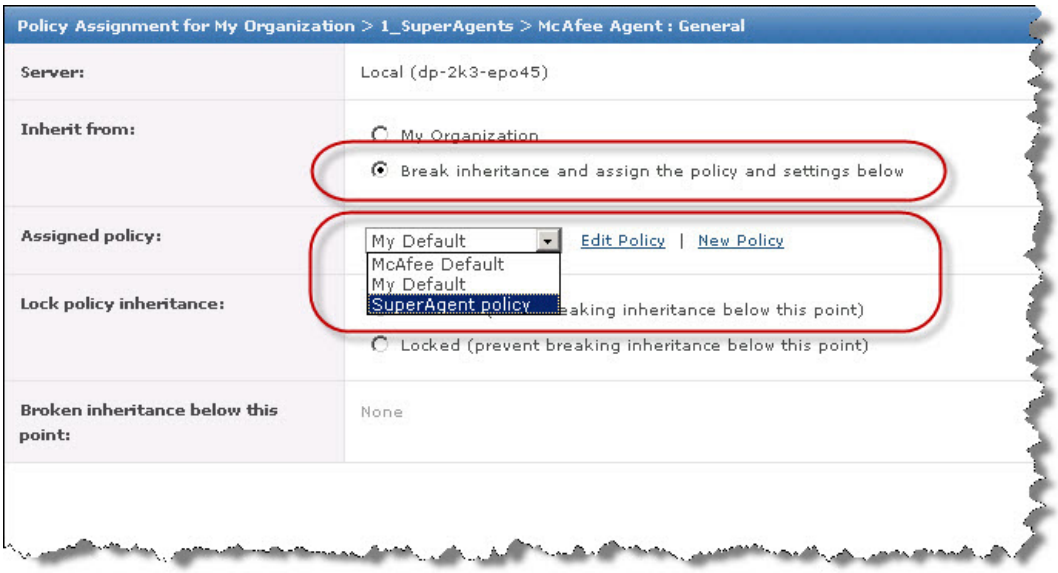
Assign the new SuperAgents policy to the new SuperAgents group.

Task

1 From the SuperAgent group you created, click the **Assign Policies** tab and select **McAfee Agent** from the Product list.

2 From the Actions column, click **Edit Assignments**. The McAfee Agent : General dialog box appears.

3 Click **Break inheritance and assign the policy and settings below**, select the SuperAgent policy you created from the Assigned Policy list, and click **Save**.



Dragging a system into the new SuperAgents group

With the SuperAgent group configured you can assign the SuperAgent policies to individual client systems simply by dragging them into that group. This converts the client systems into SuperAgents.

Change an existing system into a SuperAgent.

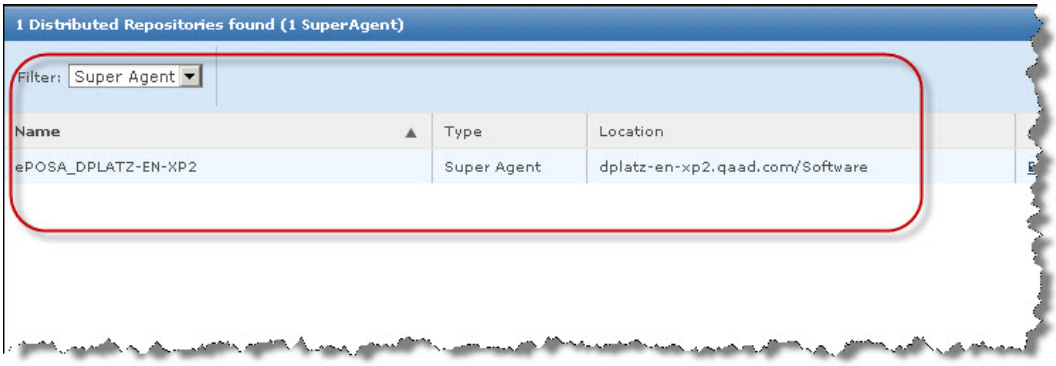
Task

1 In the System Tree, click the **Systems** tab and find the system you want to change to a SuperAgent repository.

2 Drag that row with the system name and drop it into the new SuperAgent group you created in the System Tree.

Once the system communicates with the McAfee ePO server it changes to a SuperAgent repository.

3 To confirm the system is now a SuperAgent repository, click **Menu | Software | Distributed Repositories** and select **SuperAgent** from the Filter list. The new SuperAgent repository appears in the list.



Place repositories

You need to determine how many repositories you need in your environment and where they are located. To answer these questions you need to look at your McAfee ePO server managed systems and your network geography.

Determine the following factors:

- How many nodes do you manage with the McAfee ePO server?
- Are these nodes located in different geographic locations?
- What connectivity do you have to your repositories?

Remember, the purpose of a repository is to allow clients to download the large amount of data in software updates locally instead of return to the McAfee ePO server and downloading the updates across the slower WAN links. At a minimum your repository is used to update your signature, or DAT files for McAfee VirusScan on a daily basis. In addition, your repository is used by your agents to download new software, product patches, and other content, for example Host Intrusion Prevention System content.

Typically you can create a repository for each large geographic location but there are several caveats. You must avoid the most common mistakes of having too many or too few repositories.

The following example uses updating the signature, or DAT files for VirusScan Enterprise that are released daily. The numbers used to determine if a repository is needed at a site are:

- **200 KB** — The size of the daily DAT file to download.
- **100** — The number of system agents that need to download those daily DAT files.

Example 1: Downloading directly from the central ePO server

To download the daily DAT file randomly from the central ePO server to the system agents takes the following bandwidth: 100 Agents * 200 KB file = **20 MB of bandwidth**

Example 2: Downloading the DAT file to the local repository

For the McAfee ePO server to replicate the DAT file to each repository every day takes at least **70 MB of bandwidth**.

In the previous examples, it is a waste to use 70 MB of bandwidth to download a DAT file to a repository for only 100 system agents. Those 100 system agents can download the same file using only 20 MB of bandwidth.

Calculating bandwidth of repository replication

Repository replication consumes valuable bandwidth in all environments.

If you are only replicating DAT files, the bandwidth use will be approximately 70Mb of replication per day. Agents don't use all the DAT files that are copied to the repository, but there are 35 incremental DAT files that must be available to all agents in case they are behind on DATs. In order to determine if you need a repository in a specific location, you must determine what is more costly in terms of bandwidth usage; replicating 70mb worth of data to a repository, or telling the agents to go to the next nearest repository which may not be geographically near the agents.

Calculating bandwidth for client pulls of updates

The bandwidth used to update a new product dramatically increases when updating a new product to clients.

But you can calculate the bandwidth if you know the size of the patch or product being downloaded.

At a minimum, each of your clients must download 200 Kb per day for DAT files. The following examples show how to calculate the bandwidth used for the client updates using this formula:

(*Size of update file*) x (*Number of nodes*) = Amount of data pulled per day

The following examples use this formula to calculate the amount of data pulled per day and describe if creating a local repository would reduce the bandwidth.

Example 1 — A small office in India

The small office in India needs to download the 200 Kb per day for DAT files to its 200 nodes. Using the formula:

(200 Kb) x (200 nodes) = 40 MB of data randomly pulled per day to India

In the small office in India you could add a repository but you must replicate the DAT file from the McAfee ePO server to the repository. This file replication uses approximately 70 MB of bandwidth per day over a slow WAN link could negatively impact the WAN link to India since it would occur all at once.

Instead have the agents connect across the WAN link to the next closest repository to download their DAT file updates. The next office might be in a larger office, for example the Tokyo. The agents can randomly pull their DAT files throughout the day, and their total bandwidth use is only 40 MB. See *Client task* to configure the download.

In this case do not use a repository in India.

Example 2 — A large office in Tokyo

The large office in Tokyo needs to download the 200 Kb per day for DAT files to its 4,000 nodes, using the formula:

(200 Kb) x (4,000 nodes) = 800 MB of data randomly pulled per day to Tokyo

In the large office in Tokyo with 4,000 nodes uses 800 MB of bandwidth per day just to update the DAT files alone. Since replication of the DAT file to Tokyo only uses 70 MB of bandwidth per day it is much more efficient to have a repository in the Tokyo office so all DATs can be pulled across the LAN instead of across the slower WAN link.

Example 3 — A large office in New York City

The large office in New York City needs to download a 23 MB patch update for VirusScan Enterprise to its 1,000 nodes. Using the formula:

(23 MB) x (1,000 nodes) = 23 GB of data pulled to the New York City office

This 23 MB patch is significantly larger than the 200 Kb daily DAT files. You probably have a repository in New York depending on the speed of the WAN link to New York and how quickly the patch needs to be pushed out. You might find a balance if you carefully craft your client tasks to pull updates and patches at a gradual pace instead of deploying the patch to all nodes in one day. See *Deploying products* for detailed information.

Conclusions

Some ePolicy Orchestrator users put a repository at geographic sites that have only a few dozen nodes. If your site does not have at least 200 to 300 nodes it cannot benefit from the bandwidth saved using a repository. If there is no local repository, the agents will go to the next nearest repository for their updates. This repository might be across a WAN link but it will still use less bandwidth since you don’t have to replicate the entire repository across the WAN.

The exception to this rule is if you are deploying a larger software package. For example, the VirusScan Enterprise client software is 23 MB. In this case it would be more efficient to place a repository temporarily at a smaller site so the clients software can download the 23 MB file locally. Then disable this repository once the client is rolled out.

Determine repository count

How many repositories you need depends on the hardware where the repository is installed. Most repositories can serve out files to several thousand nodes. If you are using clients as SuperAgents, they are more efficient if they are dedicated to your clients instead of sharing the SuperAgent client hardware with other applications.

There is no hard technical limit to how many nodes a repository can handle, but with a properly crafted update task for your clients, repositories can update a significant number of nodes.

The following table is an estimate of the updates a repository can handle and the hardware needed. These specifications can be influenced by many factors, for example how you update content, products, and patches.

Server hardware	Nodes updated	Dedicated or shared client hardware
Single 3 Ghz processor with 4 GB of memory	3,000	Shared with other applications
	3,000 – 7,000	Dedicated
Server class hardware, dual-quad processor and 8 GB of RAM	5,000 – 7,000	Dedicated

Disk space needed for a repository is rarely a concern with today's storage standards. Even if you checked in several McAfee endpoint products, for example Endpoint Encryption, SiteAdvisor, and Policy Auditor, your repository disk space would be in the 1 GB range.

To find out the exact size of your repository you can check the installation folder where the McAfee ePO server is located under C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software.

The following sections provide some examples of three common organization sizes and their repository size.

Example 1 — Small Organization with One Office

The small organization example has approximately 3,000 nodes of workstations and servers. It uses McAfee VirusScan Enterprise, Host Intrusion Prevention System, Encryption, and Host Data Loss Protection. It has a small data center in the same building where the devices reside so there are no WAN links and all clients are on a 100 MB LAN.

In this example you can use the primary ePO server to act as the only repository. the McAfee ePO server is always the master repository by default. For 3,000 clients, the McAfee ePO server can handle:

- Policy deployment
- Event collection
- Distributing all updates and software

Example 2 — Medium organization with four offices

The medium organization example has approximately 15,000 to 20,000 nodes. It has one data center in New York where all traffic destined for the Internet must be routed. There are four offices in the U.S. located in New York, San Francisco, Dallas, and Orlando. Each office has approximately 3,000 to 4,000 nodes with a T1 connection back to the New York office.

the McAfee ePO server, located in New York, manages all 20,000 nodes for policies and events for Endpoint Encryption, VirusScan Enterprise, Host Intrusion Prevention System, and Application Control.

A dedicated SuperAgent repository is placed in each of the three major offices that connect to the data center. These repositories are dedicated SuperAgent repositories that connect to the New York data center with medium hardware class servers, for example a single processor 3 Ghz CPU and 4 GB of RAM. Their only job is to serve out files to the McAfee Agents at each office.

Example 3 — Medium to Large Organization with Multiple Global offices

The medium-to-large organization example has 40,000 to 60,000 nodes distributed across three major regions.

The U.S. offices have one data center in New York and three additional offices across the country. Each office has approximately 7,000 nodes.

The EMEA offices have another data center in the UK with several other offices across EMEA. These other offices range from 200 nodes 3,000 nodes. The one ePO server resides in the UK data center and runs VirusScan Enterprise, Host Intrusion Prevention System, and SiteAdvisor.

The APAC offices include two smaller offices.

Region	Office	Number of nodes	Servers
U.S.	New York, Data Center	7,000	Repository
U.S.	Office 1	5,000	Repository
U.S.	Office 2	6,000	Repository
U.S.	Office 3	5,000	Repository
EMEA	U.K., Data Center	3,000	McAfee ePO server
EMEA	Office 1	200	
EMEA	Office 2	1,000	Repository
EMEA	Office 3	3,000	Repository
APAC	Office 1	500	
APAC	Office 2	300	

U.S. region servers

Put one server class client, for example dual processor 3 Ghz and 8 GB of RAM, at each site in the U.S.

EMEA region servers

Use the Systems Management Server (SMS) and install SuperAgents at each office in the EMEA since they are smaller sites. Your repository does not have to be dedicated to McAfee as long as it's not serving files to several thousand agents.

APAC region servers

There are small offices in the APAC region with slow WAN links back to the McAfee ePO server in the UK. Plus these WAN links are already saturated with traffic. This means replication from the McAfee ePO server to an APAC repository is not feasible unless it is done during off hours. This is a reasonable option if you want to put SuperAgents in APAC.

Fortunately, the APAC offices each have their own fast dedicated connections out to the Internet and do not have to route Internet traffic back to the data center in the UK. That provides two potential solutions:

- You can adjust the client tasks in APAC to have them go to the next nearest repository which may be in California.

  You must completely randomize the agents updating schedule so you spread their updates throughout the day.

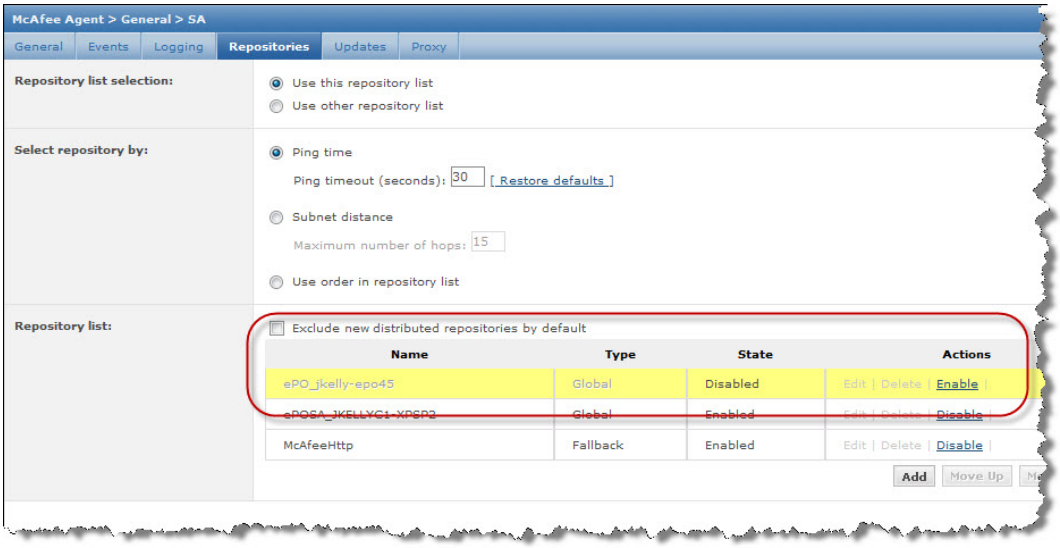
- You can put a SuperAgent in the DMZ (publicly accessible on the Internet) at one of our data centers. Then adjust the APAC client tasks forcing them to only update from this SuperAgent in the DMZ. Because the SuperAgent is local to the data center replication from ePO will be very fast. And since the agents don’t have to use a WAN link and can go straight to the Internet your slow WAN bandwidth concerns are solved.

Improve agent update performance

In large environments, the ePolicy Orchestrator server is already very busy distributing policies and collecting events. You can improve performance by changing the agent policy so agents don't pull content from the McAfee ePO server itself, the default master repository. Making this change forces the agents to use only the repositories you created manually.

> In smaller environments, where fewer nodes are managed, there's no need to make this change. The server can handle all of these tasks without impacting performance.

1. Open the Policy Catalog.
2. From the Product list, select **McAfee Agents** then from the Category list, select **General**.
3. Click **Edit Setting** and the **Repositories** tab.
4. From the Repositories list find the McAfee ePO server and click **Disable** in the Actions column.



5. Click **Save** and the McAfee ePO server repository is disabled.

Global updates

Global Updating is a powerful feature in ePO, but if it is used incorrectly it can have a negative impact in your environment. By default it is disabled when you install ePolicy Orchestrator 4.5.

Global Updating is used to update your repositories as quickly as possible whenever the master repository changes. This is great if you have a smaller environment (fewer than 3,000 nodes) with no WAN links. But Global Updates generate a lot of traffic that could impact your network bandwidth. If your environment is on a LAN and bandwidth is not a concern then go ahead and use Global Updating. If you are managing a larger environment and bandwidth is critical then disable Global Updating.

To confirm the Global Updating setting, click **Menu | Configuration | Server Settings** and select **Global Updating** from the Setting Categories list. Confirm Status is disabled. If not, click **Edit** and change the status.

How Global Updates works

If the McAfee ePO server is scheduled to pull the latest DATs from the McAfee website at 2 p.m. Eastern time, and it changes the master repository, which is always the McAfee ePO server, the server automatically starts to replicate the DATs to all your distributed repositories.

The Global Updates process works like this:

1. Content or packages are checked in to the master repository.
2. The McAfee ePO server performs an incremental replication to all distributed repositories.
3. The McAfee ePO server issues a SuperAgent wake-up call to all SuperAgents in the environment.
4. The SuperAgent broadcasts a global update message to all agents within the SuperAgent subnet.
5. Upon receipt of the broadcast, the agent is supplied with a minimum catalog version needed.
6. The agent searches the distributed repositories for a site that has this minimum catalog version.
7. Once a suitable repository is found, the agent runs the update task.

A common mistake users make with a large environment and where bandwidth is critical is thinking they should have Global Updating enabled to make sure they receive their DATs quickly. These users enable Global Updates and everything works fine. But, eventually McAfee releases an update to its VirusScan Enterprise engine which can be several megabytes compared to the 200 Kb DAT files.

Engine updates typically occurs twice per year. McAfee posts the new engine to the public site and the McAfee ePO server pulls it down and starts replicating it to the distributed repositories and starts waking up agents to receive the new engine immediately. This can saturate your WAN links and roll out an engine that you would preferred to upgrade in a staged release.

4 Agent Handlers

Agent Handlers co-ordinate work between themselves and the McAfee ePO server that communicates with the remote Agent Handlers. Agent Handlers use a work queue in the SQL database as their primary communication method. The Agent Handlers check the work queue frequently and perform the requested action.

Agent Handlers overview

Users have many questions about Agent Handlers and they are answered in the McAfee Agent Handlers white paper.

In ePolicy Orchestrator 4.0 and earlier versions, there was a single McAfee ePO server that agents could connect to and receive policy and task updates. Since the McAfee ePO server was responsible for handling every agent connecting to it, there was a limitation on the deployment size a McAfee ePO server could handle. A single McAfee ePO server could scale:

- Vertically using bigger and faster hardware
- Horizontally using more servers to distribute the load

Agent Handlers were introduced in ePolicy Orchestrator 4.5 to allow you to grow your logical ePolicy Orchestrator infrastructure horizontally, adding multiple Agent Handlers to scale agent connectivity.

Agent Handlers allow you:

- To scale your McAfee ePO server if it is overloaded handling the agent request volume
- Fail-over protection if you want agents to fail over between multiple physical servers and you do not want to cluster the McAfee ePO server
- To use topology features to manage your systems behind a Network Address Translation (NAT) or in an external network

The Agent Handler must have a high bandwidth connection to the central ePolicy Orchestrator database.

To understand what Agent Handlers do, it's important that you also understand their limitations. Agent Handlers require constant communication back to the SQL database that ePolicy Orchestrator uses. They check the McAfee ePO server database work queue approximately every ten seconds to find what tasks they need to perform. This is one of the reasons that each Agent Handler needs a relatively high speed, low latency connection to the database.

Do not use Agent Handlers to replace repositories. A repository is a simple file share meant to keep update traffic local. While an Agent Handler has repository functionality built in, it has much more intelligence and requires constant communication back to the SQL database. This constant communication can saturate the WAN link.

5 Installation and upgrade of ePolicy Orchestrator software

There are two types of ePolicy Orchestrator installations: a new installation in an environment where no previous version of ePolicy Orchestrator software has been installed, and an upgrade installation where you are replacing an existing verison of ePolicy Orchestrator software.

Before you install your ePolicy Orchestrator server software, an understanding of the hardware requirements is very important. See the *McAfee ePolicy Orchestrator 4.5 Installation Guide* and follow the preparation steps. Thorough preparation can ensure you don't have any problems during your installation.

Contents

- *Install new software*
- *Upgrade the software*
- *Move the server*
- *Move McAfee Agents between servers*

Install new software

If you are a new McAfee customer and this is your first ePolicy Orchestrator software installation, you don't have to transfer any settings from an old McAfee ePO server. Plus, you probably have a McAfee consultant with you to answer your questions and help you successfully begin using the McAfee ePO server.

Upgrade the software

There are two ways to upgrade the existing version of the McAfee ePO server. You can perform an in-place McAfee ePO server upgrade, or a clean installation of the McAfee ePO server. Both installation processes have their advantages and disadvantages. The following sections list some of the advantages and disadvantages of each upgrade.

Pros of doing an in-place ePO upgrade

The advantages of an in-place McAfee ePO server upgrade include:

- **You retain all your policies and client tasks** — This means you don't have to rebuild them and could save you time.
- **You retain your directory structure** — If you have invested a lot time building this structure an in-place upgrade may be a good idea.
- **You don't have to transfer any McAfee agents to a new server** — Since nothing changes with an in-place upgrade the upgrade is transparent to all your agents.

Cons of doing an in-place upgrade

The disadvantages of an in-place McAfee ePO server upgrade include:

- If your McAfee ePO server has been used for a long time do not transfer certain issues to the new upgrade. For example, if you ran extensive SQL scripts or altered your database in anyway outside of the normal operating procedures you might want start with a clean installation.
- Older policies might not still apply to your existing environment. Do not copy those policies during your in-place upgrade.

Assess your environments and policies periodically to confirm they still apply to your environment.

In-place upgrade tips

To make sure your in-place upgrade is successful:

- Back up your infrastructure. This includes your SQL database and any agent keys. See KnowledgeBase article KB66616 for detailed backup procedures.
- Make any hardware changes or remove any repositories that you want to decommission.
- Make sure your hardware and bandwidth meet the minimum requirements before upgrading.
- Confirm you have the required software, such as the newer version of the McAfee Agent. Remove any unsupported software. For example, Rogue System Detection or System Compliance Profiler.
- Go through your users on the McAfee ePO server and remove any unneeded accounts.
- Clean out all unused policies.
- Remove any old client tasks you no longer use. For example, old deployment tasks or old patch installation tasks. If the task is not in use remove it.
- Validate your tree and remove any agents that have not communicated with the ePO server in 14 days. In addition, remove any shell machines that were imported into ePO from Active Directory.

Shells are placeholders in the tree and do not actually have an ePO agent installed.

- Purge events that are not needed. Try to delete any events older than 60 days.
- Backup, reindex, and check your disk space on the SQL Server. Confirm you have plenty of disk space for the SQL database.
- Remove old versions of software that you are not using. For example, patches for older versions of products that are no longer used.

Replicate those patches to your distributed repositories prior to upgrading.

- Test your upgrade in a VM environment with a copy of your SQL database to make sure the upgrade works smoothly.
- Validate all your settings to confirm they are in place after the upgrade.

Move the server

There might be a time when you need to move your McAfee ePO server from one physical server to another and maintain all your settings.

For example, when your hardware is old, has failed, or is out of warranty. Or, when you upgrade your version of ePolicy Orchestrator software and you decide to upgrade your hardware as well.

Make sure you back up the following:

- The SQL database is critical. Before you do anything make sure you back up your McAfee ePO server SQL database in case something goes wrong. The database stores everything about ePolicy Orchestrator. For example, your tree structure, your product policies, administrators, events, and server settings.
- Back up these items that are outside your database:
  - Agent keys which secure the communication between the server and all your agents
  - Software checked into the master repository
  - Extensions to manage all your product policies
  - Secure Sockets Layer (SSL) certificates
  - Server settings such as communication ports

After you have backed up all of this information, follow the installation instructions in the *McAfee ePolicy Orchestrator 4.5 Installation Guide* as if it were a brand new server. Then you are left with a clean database that you replace with your original database that has all your original settings. Restore the original SQL database, agent keys and SSL certificates. For additional information, see *ePO 4.5 server backup and disaster recovery procedure*, KnowledgeBase article KB66616.

When you upgrade your McAfee ePO server from one physical server to another, make sure your new server has the same DNS name and IP address as the old server. This is the ideal situation and ultimately reduces any potential problems.

Unfortunately, one of these items may need to be changed. For example if you are changing the IP scheme a new IP address may be required, or if you change the DNS name and keep the old IP address you have to regenerate the local SSL certificates. See KnowledgeBase article KB66616. Once your database has been restored, you can turn off your old McAfee ePO server and all agents automatically start communicating with the new McAfee ePO server.

You must understand how the agents find the McAfee ePO server especially if you are moving your McAfee ePO server. The agent tries to connect to the McAfee ePO server first using the IP address, then using the fully qualified DNS name. If you move the McAfee ePO server or change its IP address the agent attempts to query the DNS to get the IP address for the DNS name. If you are going to move your McAfee ePO server you must make sure you have good DNS name resolution in your environment.

Move McAfee Agents between servers

Before the release of ePolicy Orchestrator 4.5, many customers wanted an upgrade path that would allow them to start with a new database, while retaining their old settings. Version 4.5 of the software introduced the ability to move agents from one server to another

Moving your agents from the old McAfee ePO server to the new McAfee ePO server is a compromise between copying your existing ePolicy Orchestrator SQL database to your new McAfee ePO server and having the McAfee Agents connect to the new server to populate the new, clean, database.

Using versions of ePolicy Orchestrator software prior to release 4.5, many users tried to find a compromise between starting from a new installation with a clean database but still not losing all their old settings that they created over time. This compromise was difficult because it often required extensive rebuilding of policies and tasks on the new McAfee ePO server using the process in *Move the server*. All the following steps were needed to try to mimic the older server:

1. Install a new McAfee ePO server. See *McAfee ePolicy Orchestrator 4.5 Installation Guide* for detailed instructions.
2. Export and import the following from the old McAfee ePO server to the newly built McAfee ePO server:
   - Export your product policy files in XML.
   - Export your tree structure in a txt file (ePO version 4.5 only).
   - Export any custom queries you have created.
   - Import your tree structure on your new McAfee ePO server.
   - Import the product policies and make sure they get assigned to the right groups.
   - Import any custom queries that you want to preserve.
3. All of the following items, you previously configured, must be re-created manually:
   - Client tasks including deployment, update, and on demand tasks
   - Server tasks, including the McAfee content pull and replication
   - McAfee ePO server administrators and permission sets

This is a chance to revisit policies and tasks that you have been using and could use some changing to improve efficiency.

Your new McAfee ePO server is ready to use if the previous items are completed and you have confirmed and validated your settings. Now it is time to start moving agents to the new McAfee ePO server. The traditional way of doing this was to redeploy a new McAfee Agent from the new McAfee ePO server which would point your agents to the new server. This is inefficient because you already have a working agent on all your clients, but the agents are still pointing to your old McAfee ePO server. To fix this use the Transfer Systems feature on ePolicy Orchestrator 4.5, or later, servers to move your agents from one McAfee ePO server to another.

Exporting and import the ASSC keys

You must export the agent-server secure communication (ASSC) keys from the old server to the new server before moving your clients to the new McAfee ePO server. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for detailed agent-server secure communication key export and import instructions.

Using Transfer Systems feature on ePolicy Orchestrator 4.5, or later

You can move agents from your old McAfee ePO server to your new McAfee ePO server using the Transfer Systems task. The Transfer Systems task gives the existing agent a new sitelist.xml file that points to the new McAfee ePO server. But, both the old and the new McAfee ePO servers must be running ePO version 4.5, or later.

You cannot, for example, move agents from an ePolicy Orchestrator 4.0 server to an ePolicy Orchestrator 4.5 server.

You must configure a registered server before you can use the Transfer Systems feature. See *McAfee ePolicy Orchestrator 4.5 Product Guide*, *Setting up registered servers* for details.

The Transfer Systems task is one of the most powerful and useful features of ePolicy Orchestrator 4.5. It allows you to:

- Stage and thoroughly plan your agent moves so you can test their settings during an appropriate change control window.
- Test your changes on a development McAfee ePO server before rolling out the changes to the production environment. For example, you can make changes on your test McAfee ePO server and move a group of live production agents to your test server to see the results. When done, you can easily transfer those agents back to the original production McAfee ePO server.

See *McAfee ePolicy Orchestrator 4.5, Product Guide* for details on using Transfer Systems.

Using Transfer Systems

Use the ePolicy Orchestrator 4.5 Transfer Systems task to move your agents from the old McAfee ePO server to the new McAfee ePO server.

Before you begin

Transfer Systems is only available on ePolicy Orchestrator 4.5, or later.

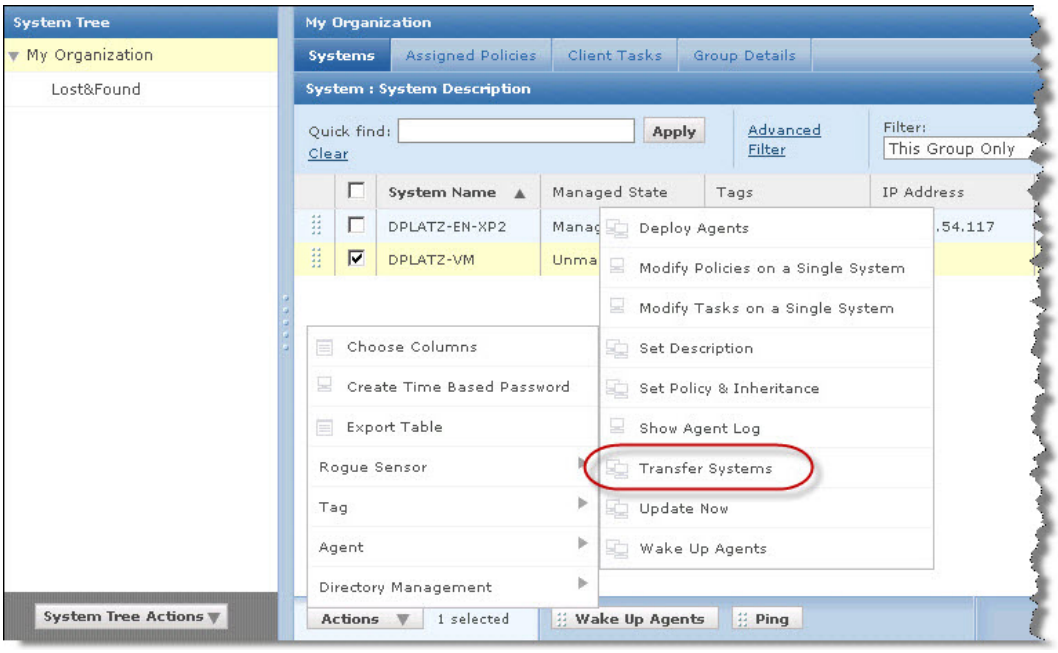
See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details on using Transfer Systems.

Use the ePolicy Orchestrator 4.5 Transfer Systems task.

Task

1. On the old McAfee ePO server, configure the new McAfee ePO server as a registered server. See *McAfee ePolicy Orchestrator 4.5 Product Guide*, *Setting up registered servers* for details.
2. On the old McAfee ePO server, click **Menu** | **Systems** | **System Tree** and the **Systems** tab to open a list of systems.

3 Select the systems to move to the new McAfee ePO server and click **Actions | Agents | Transfer Systems**. The Transfer Systems dialog box appears.



4 Select the server from the drop-down menu and click **OK**.

Once a managed system has been marked for transfer, two agent-server communications must occur before the system is displayed in the System Tree of the target server. The length of time required to complete both agent-server communications depends on your configuration. The default agent-server communication interval is one hour.

6 McAfee Agent

The McAfee agent is the liaison between all point-products and the McAfee ePO server. This 5 MB executable file is not a security product on its own; instead it communicates to all the McAfee and partner security products and passes the appropriate information to and from the McAfee ePO server.

Contents

- *Agent functionality*
- *Deploying agents*

Agent functionality

Understanding the McAfee Agent functionality and how it work with the McAfee ePO server is very important to effectively configure and manage your environment.

The McAfee Agent core functionality includes:

- Handling all communication to and from the McAfee ePO server and passing that data to the endpoint products.
- Pulling all product policies from the McAfee ePO server and assigning the policy to the appropriate products that is installed on the endpoint clients.
- Pulling all client tasks from the McAfee ePO server and passing it to the appropriate products
- Deploying all content such as anti-virus signatures, auditing checks, and engines
- Deploying all new product upgrades, new products, patches, and hotfixes
- Upgrading itself silently with no reboot required when a new agent is released

The terms *McAfee Agent* and *agent* are used interchangeably.

Once an agent is installed on a system, you never need to use a third-party deployment tool to update anything on that client.

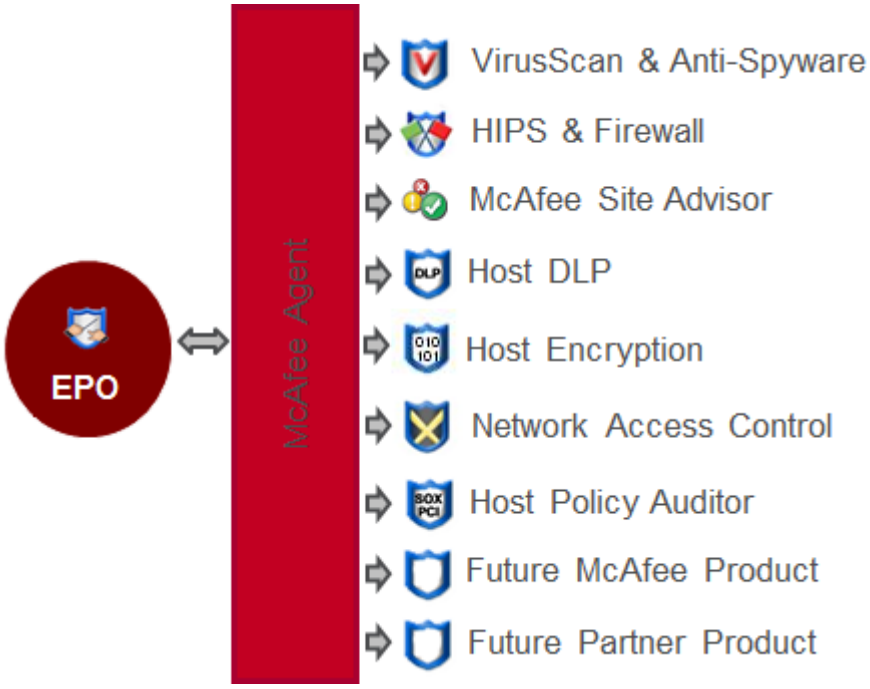


Figure 6-1 One agent to communicate with many products

McAfee Agent modularity

The advantage to the agent design is modularity. This modular design allows you to add new security offerings to your environment, as your needs change, using the same agent framework. McAfee can build a standard on how policies, events, and tasks, for example, are passed to endpoint solutions. You never have to worry about communication or which ports to open when you add a new product such as Host Data Loss Protection to your endpoint. All those items are controlled by the agent. Agent modularity also allows the development teams to work more efficiently and integrate new products into the McAfee ePO server faster. The advantages to this modular architecture are:

- One component provides communication back to the server instead of multiple solutions with their own proprietary communication language.
- You have the flexibility to choose which products fit your organization instead of being dictated by your security vendor.
- You can add controlled patching of individual products. For example, if there is a patch for the Endpoint Encryption product VirusScan Enterprise cannot be affected by the patch.
- The patch process is consistent across all products since the McAfee ePO server controls the process.
- You add new products as they are released by McAfee and its partners.
- You can leverage the same McAfee agent for partner products instead of adding more overhead. See Partner Products for details.

Deploying agents

You can deploy the McAfee Agent multiple ways. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details. But there are a few concepts that can help you to understand.

The McAfee Agent is a 5 MB executable file that can simply be executed manually or more commonly deployed on a larger scale to hundreds or thousands of nodes. The agent can be deployed using:

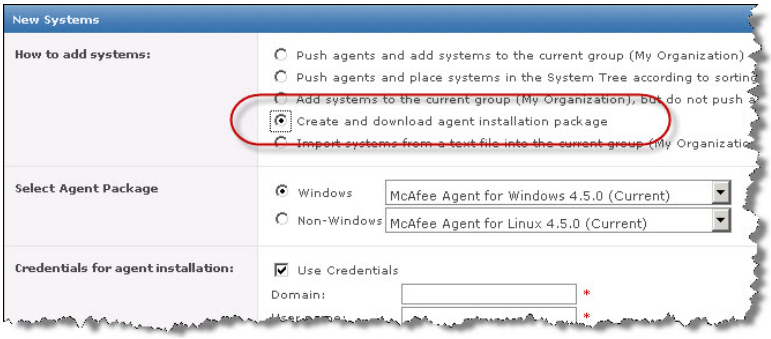
- A logon script
- Manual execution
- The McAfee ePO server
- Third-party tools
- An image with the agent as part of the image

You must use the specific McAfee agent executable file obtained from the McAfee ePO server in your environment. Each agent is created dynamically during the initial installation of your McAfee ePO server. There are a few things inside your agent executable that are unique to your environment, which is why the agent can only be obtained from your organization's ePolicy Orchestrator server. You cannot download a blank McAfee Agent from the McAfee download site and start deploying it.

Obtain a copy of your McAfee Agent.

1 Click **Menu | System | System Tree**, from the System Tree pane, click **System Tree Actions | New Systems**. The New Systems dialog box appears.

2 Click **Create and download agent installation package**, complete the credentials needed, and click **OK**.


New Systems
How to add systems:
Push agents and add systems to the current group (My Organization)
Push agents and place systems in the System Tree according to sorting
Add systems to the current group (My Organization), but do not push
Create and download agent installation package
Import systems from a text file into the current group (My Organizatio
Select Agent Package
Windows
McAfee Agent for Windows 4.5.0 (Current)
Non-Windows
McAfee Agent for Linux 4.5.0 (Current)
Credentials for agent installation:
Use Credentials
Domain:

3 From the Download File dialog box, save the files to a local machine.

If you look inside this executable file you can see what makes it unique. Your custom package has the communication keys for your specific ePolicy Orchestrator server and a sitelist.xml file. Without these keys the agents cannot talk to your specific ePolicy Orchestrator server.

cleanup.exe 1/13/2010 5:45 PM
FrmInst.exe 1/13/2010 5:45 PM
MFEagent.msi 1/13/2010 5:45 PM
reqseckey.bin 1/13/2010 5:45 PM
SiteList.xml 5/10/2010 10:37 AM
srpubkey.bin 1/13/2010 5:45 PM

The sitelist.xml file tells all your agents how to find the McAfee ePO server using the IP address and DNS name. This is important because there are many situations when this file becomes outdated. For example, if you rename your ePolicy Orchestrator server or give it a new IP address, or if you have multiple ePolicy Orchestrator servers you will have multiple unique McAfee Agent files designed to communicate with the ePolicy Orchestrator server where is was created.

If you gave this custom McAfee Agent to your desktop team a year ago, it is probably outdated. It becomes outdated if, for example you have made changes to your ePolicy Orchestrator server such as rebuilding it with a new IP address, or checked in a newer version of the McAfee Agent into your server.

Keep the agent file up to date

It is important to download the latest agent file and give it to the appropriate teams so they have the latest agent file version for new deployments. Make sure you know who has the agent executable in your environment and always control it by choosing a central share that you update every time you make changes to your agent.

Deploy from the McAfee ePO server

The quick and easy way to deploy the agent is directly from the McAfee ePO server. This method works well if you have a smaller environment and good control over the environment with the appropriate administrator rights. You can also solve situations where a few agents need to be deployed to new machines on the network. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details.

Troubleshooting agent deployment from ePO

The McAfee ePO server requires local administrator rights to deploy agents remotely. Plus the machine you are deploying to must have:

- Admin$ share enabled
- Netbios enabled
- No firewall blocking inbound communications

An easy way to troubleshoot the agent deployment is by attempting to connect to the potential agent from the McAfee ePO server itself. To test the connection use the Microsoft Windows Run prompt and type:

```
\\<machinename>\
```

Where "<machinename>" is the name of the machine being tested.

If you can connect to the share using credentials, you know the McAfee ePO server can deploy an agent to the target machine. If you cannot open this share, there is no way the McAfee ePO server can deploy an agent remotely.

Failure to connect to the target machine is usually because of a credential failure or a firewall that is blocking netbios communication. Confirm you have the appropriate rights on the target machine before trying to deploy the agent from the McAfee ePO server.

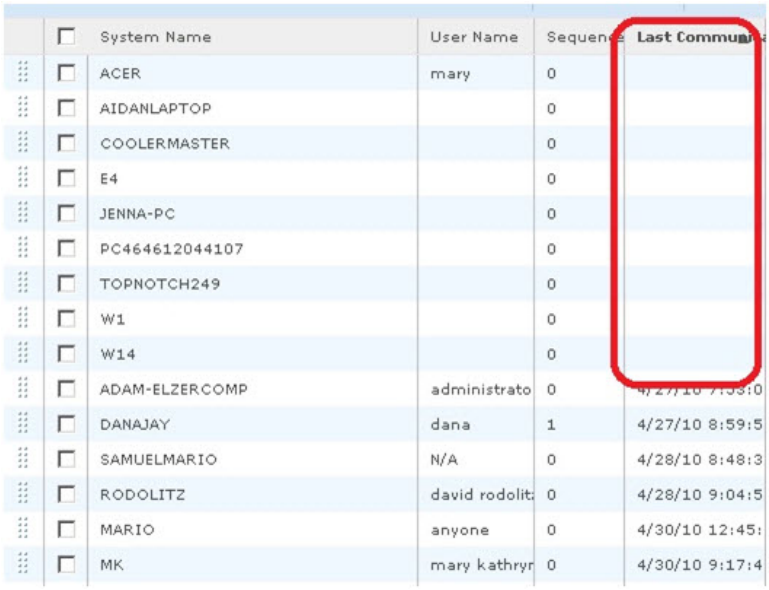
Synchronize with Active Directory

You can use deployment from the McAfee ePO server on its own or with Active Directory (AD) synchronization.

ePolicy Orchestrator can import your machines from AD and subsequently push agents from the McAfee ePO server using the remote deployment functionality. This can be scheduled using the McAfee ePO server tasks to run at specific intervals, such as once per day. This process requires the following:

- The machines in your AD tree must be well maintained. This is not always the case in many larger organizations. Machines need to be deleted and placed into appropriate containers in AD for ePolicy Orchestrator to properly mirror your AD structure.
- You must have the proper credentials, have the admin$ share enabled, and there must be no local firewall blocking the netbios ports on the destination client for the push from ePolicy Orchestrator to work properly.
- The target machine must be turned on. Just because the machine exists in Active Directory does not mean it is turned on and active on your network. During the push from the McAfee ePO server if the machine is not connected to the network then the push fails.

Agent deployment from the McAfee ePO server works well as long you have a well maintained AD structure. If not, you will end up with excessive shells or placeholders in your System Tree. These shells are machines that have been imported from your AD server but have never received a McAfee Agent. The following figure is an example of shell machines without agents installed.



System Name	User Name	Sequence	Last Communication
ACER	mary	0	
AIDANLAPTOP		0	
COOLERMASTER		0	
E4		0	
JENNA-PC		0	
PC464612044107		0	
TOPNOTCH249		0	
W1		0	
W14		0	
ADAM-ELZERCOMP	administrato	0	4/27/10 7:53:0
DANAJAY	dana	1	4/27/10 8:59:5
SAMUELMARIO	N/A	0	4/28/10 8:48:3
RODOLITZ	david rodolit	0	4/28/10 9:04:5
MARIO	anyone	0	4/30/10 12:45:
MK	mary kathryn	0	4/30/10 9:17:4

Shell machine appear in the previous figure with no date in the Last Communication column.

Make sure your environment is properly covered with McAfee Agents to avoid these shell machines. These shell machines:

- Leave your System Tree cluttered and unorganized
- Should be deleted on a regular basis using an ePolicy Orchestrator server task, if needed
- Skew your reports and queries because they are only placeholders for machines, not machines that are actively talking to the McAfee ePO server

You can filter out these shells in your reports but it is much better to make sure your environment is properly covered with McAfee Agents.

Deploy the agent using third-party tools

You can deploy the McAfee agent using a third-party tool that you already use for patches and new product deployments.

Using third-party tools is not a requirement, but your organization might have strict policies that dictate how products are deployed for consistency and change control reasons. Some common deployment tools include:

- Microsoft SCCM (formerly known as SMS)
- IBM Tivoli
- Novell Zenworks
- BMC Client Automation (formerly Marimba)
- Simple logon scripts

The process used to deploy the agent for the first time using these third-party tools is very straightforward. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details.

The McAfee Agent file, named FramePkg.exe, has several installation switches to choose from. At a minimum you need to tell the agent to install itself and optionally, do not show the installation GUI to the end user using the `/s` switch. Following is an example of this command:

```
FramePkg.exe /install=agent /s
```

Make the agent part of your image

An installed McAfee Agent on every system in your environment ensures ePolicy Orchestrator compliance in your organization. The best strategy for ePolicy Orchestrator compliance is to make your systems all receive the McAfee Agent during the imaging process.

To obtain complete ePolicy Orchestrator compliance requires planning and communication with your build team to ensure the McAfee Agent is part of every system from the beginning. That also ensures any required McAfee product and associated policy is pulled from the McAfee ePO server by the agent on your machines. This ensures maximum coverage and is imperative for environment security. There are two options when making the agent part of your build process:

- Option 1 — Include the agent in your Windows image before freezing or finalizing the image.
- Option 2 — Run the agent executable after your image is created using a repeatable script.

Both of these options install the McAfee Agent on the managed systems. Once you have agents as part of your imaging process they automatically call in to the McAfee ePO server within 10 minutes and receive whatever policy and products are dictated by ePolicy Orchestrator. At this point you can either allow your newly built machines to call into the McAfee ePO server and receive a client task to install the proper McAfee endpoint products, or you can make the endpoint products part of your build process and included them in the original image.

Here are some pointers to help you decided which option to use:

- The initial pull of multiple McAfee endpoint products can take a lot of bandwidth. If you have bandwidth constraints make the products part of your original image.
- If your build process occurs on a network where your imaged machines do not have network connectivity to the McAfee ePO server then make the endpoint products part of your imaging process.
- It takes up to 10 minutes for the agent to call into the McAfee ePO server on the first communication. Plus, it will take several more minutes to download, install, and update the VirusScan Enterprise products using a client task. If timing is a concern, and you don't want to wait 15 or 20 minutes for the products to install, make the McAfee products part of your image.

Make sure you delete the agent GUID before freezing the image if you choose option 1.

Confirm you deleted the agent GUID before freezing the image

If you choose option 1, *Include the agent in your Windows image* it can cause one of the most common problems seen in ePolicy Orchestrator, not resetting the Agent GUID. This causes the systems to not appear in the ePolicy Orchestrator directory.

To solve this problem, you must make sure you delete the agent GUID before freezing the image when you make the agent part of your image. If this registry key is not deleted, countless machines will use the same GUID. This has a very negative effect in your environment. See *McAfee ePolicy Orchestrator 4.5 Product Guide* and McAfee KnowledgeBase article KB56086.

Failure to delete the McAfee Agent GUID from the registry before finalizing your image can be difficult to manage in larger environments because there may be several imaging teams involved or an outsourcing organization building the images. Make sure your imaging teams understand how to follow the procedure outlined in KB56086. If you have a suspicion that there is a duplicate GUID problem in your environment, see *Determining if you have a duplicate GUID problem*.

7 Organizing your System Tree

Your System Tree is a very important feature of your McAfee ePO server and you can configure the System Tree hierarchy in multiple ways.

Contents

- *Your System Tree*
- *Use Active Directory synchronization*
- *Dynamically sorting your machines*

Your System Tree

Your System Tree is the structure that dictates:

- How your policies for different products are inherited
- How your client tasks are inherited
- What groups your machines go into
- What permissions your administrators have to access and change the groups in the System Tree.

If you are creating your tree for the first time, the primary options available for organizing your systems dynamically are:

- Using Active Directory (AD) synchronization
- Dynamically sorting your machines

AD synchronization can be used with dynamic tree sorting, but ideally try to pick one or the other. There can be some confusion and conflicts when using both.

See *McAfee ePolicy Orchestrator 4.5 Product Guide* for System Tree configuration details.

Use Active Directory synchronization

Active Directory synchronization allows you to pull your systems and organizational units from your AD structure and mirror them in ePolicy Orchestrator. This is an ideal option if your AD structure is nicely organized for you by business unit, machine type, and others. Unfortunately, AD structure is not always well organized.

Dynamically sorting your machines

To dynamically sort your machines into your ePolicy Orchestrator System Tree use a combination of system criteria, such as machine name or IP address, to dynamically move machines into their appropriate group in your ePolicy Orchestrator System Tree.

This requires you to create some basic groups for your tree structure. For smaller organizations your tree might not be that complex and contain only a few groups. For larger organizations you could create the following building blocks and assess the pros and cons of a few designs:

- **GEO** — Geographic location
- **NET** — Network location
- **BU** — Business unit
- **SBU** — Sub business unit
- **FUNC** — Function of the system (web, SQL, app server)
- **CHS** — Chassis (server, workstation, laptop)

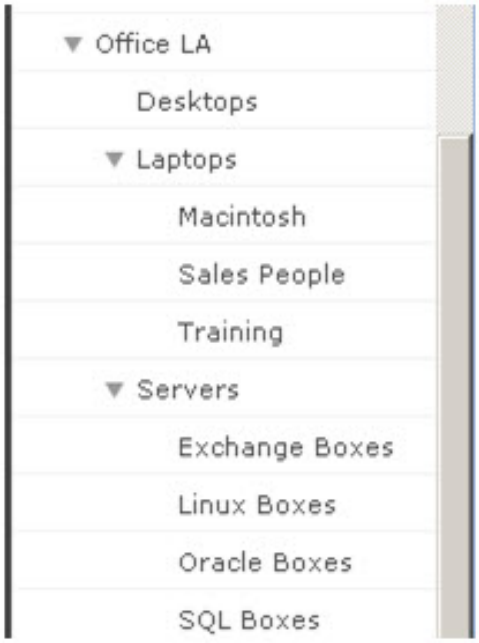
After you decide on the basic building blocks for groups in the tree you need to determine which building blocks to use and in which order based on the following factors:

- **Policy Assignment** — Will you have many different custom product policies to assign to groups based on chassis or function? Will certain business units require their own custom product policy?
- **Network Topology** — Do you have sensitive WANs in your organization that can never risk being saturated by a content update? Or do you only have major locations and this is not a concern?
- **Client Task Assignment** — When it comes time to create a client task, such as an on-demand scan, will you need to do it at a group level, such as a business unit, or system type, like a web server?
- **Content Distribution** — Will you have an agent policy that specifies certain groups must go to a specific repository for content?
- **Operational Controls** — Will you need specific rights delegated to your ePolicy Orchestrator administrators that will allow them to administer specific locations in the tree?
- **Queries** — Will you need many options when filtering your queries to return results from a specific group in the System Tree. This is another factor that may be important when designing your tree.

After you choose the basics for your tree structure, create a few sample trees and look at the pros and cons of each design. There is no right way or wrong way to build your tree, just pluses and minuses depending on what you choose. Following are a few of the most common tree designs users tend to use:

- GEO -> CHS -> FUNC
- NET -> CHS -> FUNC
- GEO -> BU -> FUNC

The following example is an example of GEO -> CHS -> FUNC, or geographic location, chassis, and function.


Office LA
Desktops
Laptops
Macintosh
Sales People
Training
Servers
Exchange Boxes
Linux Boxes
Oracle Boxes
SQL Boxes

8 Policies and packages

Policies are the settings that govern each product on the endpoint. Packages are the binaries that can be deployed by the McAfee Agent to your endpoints.

Policies include the settings for any supported products from McAfee VirusScan Enterprise to McAfee Endpoint Encryption. These policies include every checkbox and setting that dictates what the endpoint product does on each one of your systems.

Deployment packages are the actual binaries deployed by the McAfee Agent to your endpoint systems. This includes deploying a full product, such as, a new version of VirusScan Enterprise or McAfee SiteAdvisor to your endpoint systems. Policies and packages **do not** rely on each other and are not connected. In other words, just because you want to manage VirusScan Enterprise policies with ePolicy Orchestrator does not mean you have to *deploy* VirusScan Enterprise with ePolicy Orchestrator.

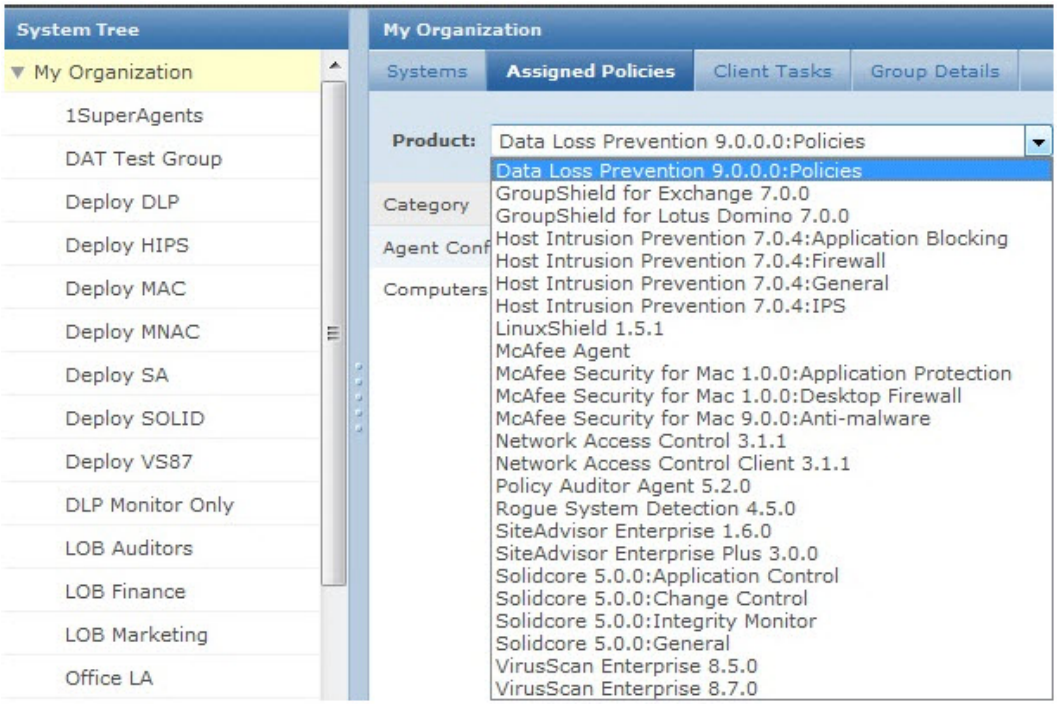
Contents

- *Manage policies*
- *McAfee agent policy*
- *Deploying packages*

Manage policies

A policy is a collection of settings that you create and configure, then enforce. Policies ensure that the managed security software products are configured and perform accordingly. ePolicy Orchestrator manages policies for all point-products that the McAfee Agent can manage.

The following example shows all the products in the drop-down list that the McAfee ePO server can manage.



This is not an exhaustive list and new products are constantly being added as McAfee expands its solution portfolio. Because of the McAfee ePO server's modular architecture, you can instantly add new product policies for management by ePolicy Orchestrator by checking in a product extension. An extension is a zip file, released by McAfee or a partner vendor, that you simply check into ePolicy Orchestrator so you can manage a product's policies. See McAfee Security Innovation Alliance (SIA) for a list of partner vendors.

By default all policies are inherited from the "My Organization" level, the highest point in the System Tree. This means all policies for all products flow downward into the groups and subgroups below it. Always set your policies at the My Organization level and let your policies flow downward.

Try to find a middle ground for all your policies that apply to as many systems as possible in your System Tree. This might not be realistic for all products, for example complex products like VirusScan Enterprise or Host Intrusion Prevention System. But, less complex policies can apply to all systems, for example the McAfee Agent policies govern all the settings for the McAfee Agent itself.

McAfee agent policy

The McAfee Agent policy is a universal policy that applies to every system in your environment, becasue the agent is required for all other point-products.

See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details about the McAfee Agent policy default settings.

Agent to server communication interval (ASCI)

The agent-to-server communication interval (ASCI) dictates how often every McAfee Agent calls the McAfee ePO server, and is one of the most important settings under the agent policy.

The ASCI is set to 60 minutes by default and:

- Collects and sends its properties to the McAfee ePO server or Agent Handler
- Checks to see if any policy changes or client tasks have occurred on the McAfee ePO server and pulls down the changes to the client

For example, if any change is made to a policy for a point-product managed by ePolicy Orchestrator, such as VirusScan Enterprise, Endpoint Encryption, or Host Data Loss Protection, at the ASCI time that change is pulled down by the agent and applied to the endpoints.

Ask how often changes occur for endpoint policies on your McAfee ePO server. For most organizations, once your policies are put in place they do not change very often. Some organizations change an endpoint policy less than once every few months. That means a system calling in every 60 minutes looking for a policy change (approximately eight times in a typical work day) might be excessive. If the agent does not find any new policies to download it will rest until the next ASCI then check again at its next scheduled check-in time.

When determining your ASCI, the concern is not necessarily a waste of bandwidth. ASCI communications are extremely light and only a few kilobytes per ASCI. The concern is the strain put on the McAfee ePO server with every communication from every agent in larger environments. All of your agents need at least two communications per day with the McAfee ePO server. This requires a 180 – 240 minute ASCI in most organizations.

For smaller organizations, less than 10,000 nodes, the ASCI number is not a concern and can be as frequent as 60 minutes. But for larger organizations you want to make sure you do not keep the default setting of 60 minutes, and use the 3 – 4 hour range for your ASCI.

For a much larger organization, 60,000 nodes or greater, the ASCI setting is much more important. If your McAfee ePO server is not having performance issues, you can use the 4 hour ASCI interval. But if there are any performance issues consider increasing your ASCI to 6 hours, possibly even longer. This significantly reduces the number of agents that are simultaneously connecting to the McAfee ePO server and improves performance on the server.

You can determine how many connections are being made to your McAfee ePO server by using the ePO Performance Counters. See *Determining if your server has performance problems*.

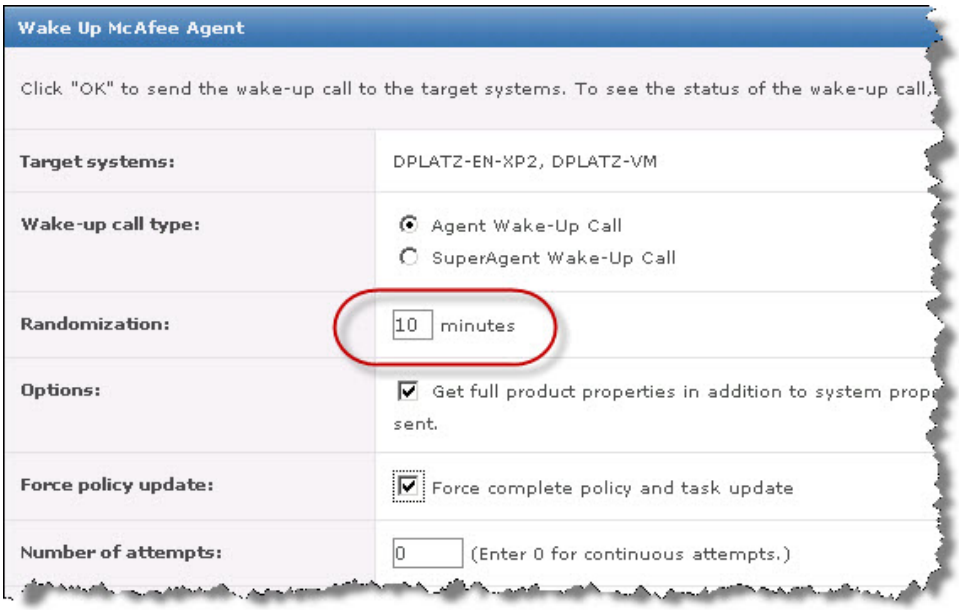
The following table provides ASCI basic guidelines.

Node count	Recommended ASCI interval
100 – 1,0000	60 – 120 minutes
10,000 – 50,000	120 – 240 minutes
50,000 or more	240 – 360 minutes

Sending a policy change immediately

If you need to send a policy change or add a client task you execute an agent wake-up call. The agent wake-up call is a communication from the McAfee ePO server to agents or a group, that you can manually choose, that asks the agent to perform its ASCI immediately. Use the agent wake-up call only in critical situations and not haphazardly because they can put a resource strain on the McAfee ePO server while they are being performed. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details.

If you need to wake-up thousands of systems, stagger the process by waking up a few thousand at a time. You should also randomize the wake-up call for a few minutes to lessen the strain on the McAfee ePO server. The following figure shows the randomization setting.


Wake Up McAfee Agent
Click "OK" to send the wake-up call to the target systems. To see the status of the wake-up call,
Target systems:
DPLATZ-EN-XP2, DPLATZ-VM
Wake-up call type:
Agent Wake-Up Call
SuperAgent Wake-Up Call
Randomization:
10 minutes
Options:
Get full product properties in addition to system prop
sent.
Force policy update:
Force complete policy and task update
Number of attempts:
0 (Enter 0 for continuous attempts.)

Configuring ASCI

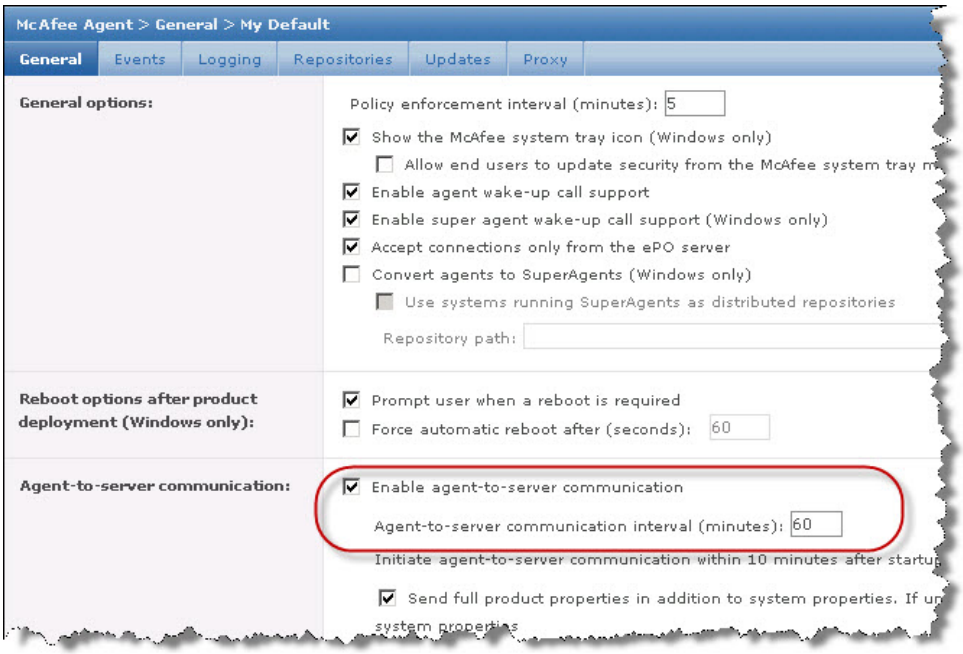
Configure the ASCI to determine how often every McAfee Agent calls the McAfee ePO server

The ASCI is set to 60 minutes by default. If that interval is too frequent change the interval.

Task

1 Click **Menu | Policy | Policy Catalog**, then select **McAfee Agent** from the Product list and **General** from the Category list.

2 Click the **General** tab, and type the **Agent-to-server communication interval** as shown in the following figure.


McAfee Agent > General > My Default
General
Events
Logging
Repositories
Updates
Proxy
General options:
Policy enforcement interval (minutes): 5
Show the McAfee system tray icon (Windows only)
Allow end users to update security from the McAfee system tray
Enable agent wake-up call support
Enable super agent wake-up call support (Windows only)
Accept connections only from the ePO server
Convert agents to SuperAgents (Windows only)
Use systems running SuperAgents as distributed repositories
Repository path:
Reboot options after product deployment (Windows only):
Prompt user when a reboot is required
Force automatic reboot after (seconds): 60
Agent-to-server communication:
Enable agent-to-server communication
Agent-to-server communication interval (minutes): 60
Initiate agent-to-server communication within 10 minutes after startup
Send full product properties in addition to system properties. If up
system properties

3 Click **Save**.
If you need to send a policy change or add a client task immediately, you execute an agent wake-up call. See *Agent to server communication interval (ASCI)*, *Sending a policy change immediately*.

Configuring the policy enforcement interval

It is very important to understand the policy enforcement interval under the agent policy. This is especially important if you have underpowered client machines that need every advantage they can get when it comes to saving hardware resources.

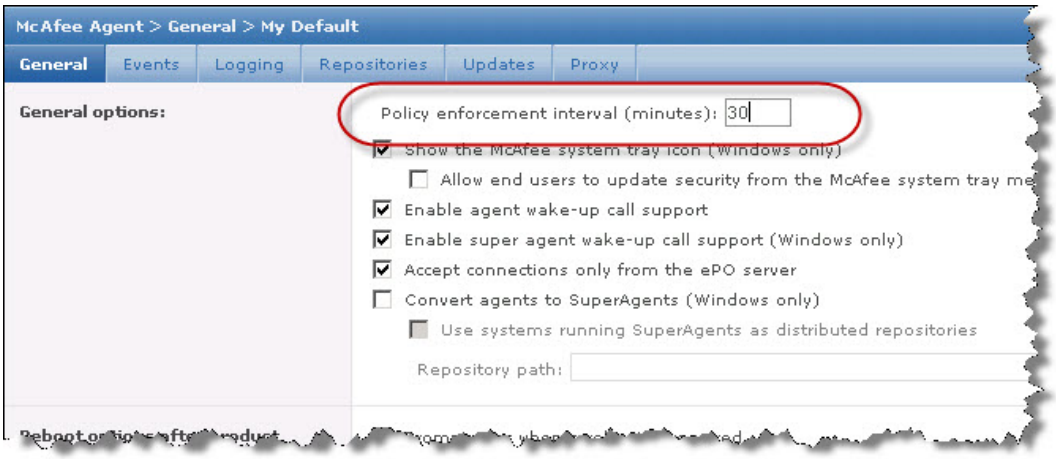
Policy enforcement is purely local and does not require communication with the McAfee ePO server. Policy enforcement makes the agent compare the last known product policy pulled from the McAfee ePO server to the current policy on the client. For example, if an end user had the ability to disable VirusScan Enterprise on their machine and the last policy pulled from the McAfee ePO server stated that VirusScan Enterprise must be enabled the agent will enable VirusScan Enterprise at this enforcement interval.

The default Policy enforcement interval is 5 minutes. That setting requires the agent to wake up 96 times in an average 8 hour work day to enforce all point-product settings. This can be excessive on legacy machines which are not as robustly configured as typical desktop workstations. If you slightly increase this interval it will reduce the amount of local enforcement that occurs on each client. For example, increasing this interval to 15 or 30 minutes will significantly reduce the amount of local enforcement that occurs on a daily basis.

Adjust the Policy Enforcement Interval for the McAfee Agent.

1 Click **Menu | Policy | Policy Catalog**, then select **McAfee Agent** from the Product list and **General** from the Category list.

2 Click the **General** tab, and type the **Policy enforcement interval** as shown in the following example.


McAfee Agent > General > My Default
General
Events
Logging
Repositories
Updates
Proxy
General options:
Policy enforcement interval (minutes): 30
Show the McAfee system tray icon (Windows only)
Allow end users to update security from the McAfee system tray me
Enable agent wake-up call support
Enable super agent wake-up call support (Windows only)
Accept connections only from the ePO server
Convert agents to SuperAgents (Windows only)
Use systems running SuperAgents as distributed repositories
Repository path:

Deploying packages

Packages are the binaries or files that can be deployed to an endpoint. All packages that could be deployed from the McAfee ePO server are located in the master repository.

You do not have to check all packages into the master repository if you do not plan to deploy them with the McAfee ePO server. If you plan to use a third party tool to deploy McAfee products, you do not need to check in the package into the master repository. All content that is updated frequently, for example patches and signature files, can be checked in manually or checked in using an automated server task.

ePolicy Orchestrator tracks package versions, both major and minor, and ePolicy Orchestrator version 4.5, and later, allows packages to be checked into all three ePolicy Orchestrator repository branches: Current, Previous and Evaluation.

The branch a package is checked into is selected at the time the package is checked in and can be modified manually.

The multiple branch feature in ePolicy Orchestrator allows multiple versions of the same package, for example Virus Scan Enterprise, in the same repository. This allows installation of that package on a subset of the environment for testing prior to production rollout.

The multi-branch feature for packages is not enabled by default. Enable multiple branches in your repository.

Task

For option definitions, click **?** in the interface.

1 Click **Menu | Configuration | Server Settings**, then in the Settings Category pane click **Repository Packages**, The following dialog box appears.

2 Click **Edit** and change the default from **No** to **Yes** and save the change.

Once configured, the branch used for a particular installation can be selected when configuring the Client Task

9 Client tasks

Client tasks run on the clients and are typically scheduled to run at a specific time. They are different from policies because they are an action that the client must perform at a predetermined time.

Many of the tasks are specific to certain products, if you have their extensions checked in to ePolicy Orchestrator. But the major tasks dedicated to the McAfee Agent are:

- **Product deployment** — Tells the agent which products you want it to deploy to the client
- **Product update** — Uses the McAfee Agent update content such as VirusScan signatures, engine, or product patches

Client tasks can be set at a group or machine level and always inherits to the group or machine below them. Always try to set your client tasks at the highest point of your directory tree, like the My Organization level. This reduces the number of tasks you have to manage and keeps your administration overhead to a minimum.

Contents

- *Deploy products*
- *Updating products*

Deploy products

Product deployment tells the agent which products you want deployed to the client and when.

To deploy a product you must create a task and either link it to policy enforcement or schedule it to occur. The agent deploys the products in the order you specify until all products are installed using the schedule you specify.

Many of the tasks are specific to certain products, for example VirusScan Enterprise or SiteAdvisor if you have their extensions checked into ePolicy Orchestrator. But there are two tasks that are dedicated to the McAfee Agent. Those two tasks are Product deployment and Product update. See *Updating products* for detailed product updating information.

You also have the option of running this task at every policy enforcement interval. This feature can be confusing. See *Configuring the policy enforcement interval* for details. Policy enforcement occurs every five minutes by default on all clients based on the McAfee Agent policy. Policy enforcement is purely local and does not need to communicate with the McAfee ePO server. Policy enforcement makes the agent compare the last known product policy pulled from the McAfee ePO server to the current policy on the client. By enabling this feature the agent confirms the products you want installed by this task are still installed at every policy enforcement interval. This is a good way to make sure no changes occur on the endpoint by the end user. If the end user somehow removes or alters a point product the agent reinstalls it based on this option.

It is not necessary to enable this option if your schedule is properly built. See *Scheduling product deployment with randomization*.

Configuring which products are deployed

Configure the agent client to deploy a product. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details.

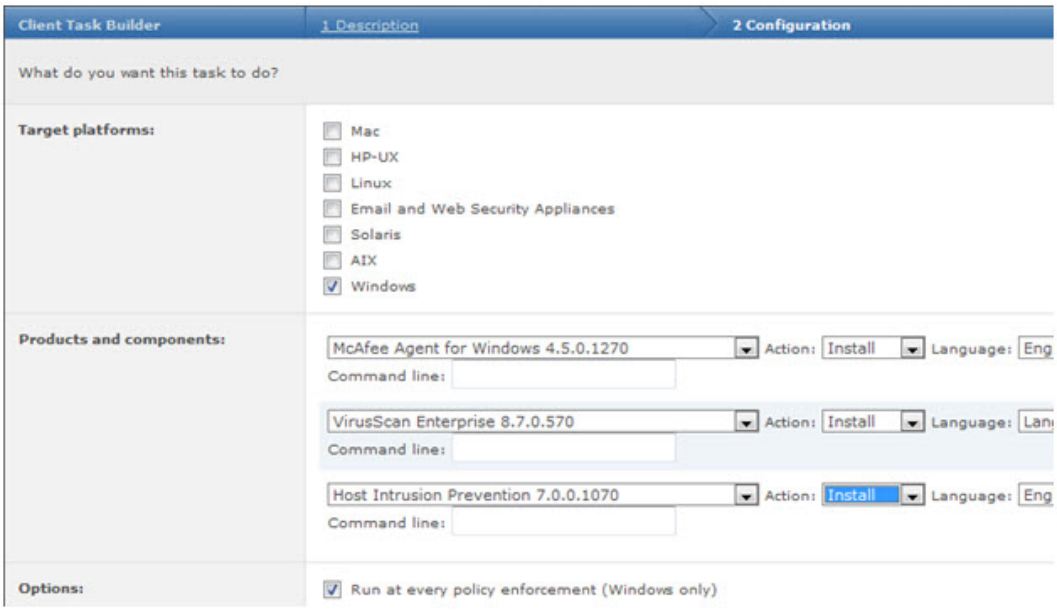
Task

1 Click **Menu | Systems | System Tree | Client Tasks**, then select a group in the System Tree.

2 Click **Actions | New Task**. The Client Task Builder wizard opens.

3 Type a name, select **Product Deployment** from the list, and click **Next**. The Client Task Builder page appears.

4 Configure the **Target platforms** and **Products and components**.



5 Optional. Click **Run at every policy enforcement**.

6 Click **Next** to configure scheduling product deployment with randomization.

Schedule product deployment with randomization

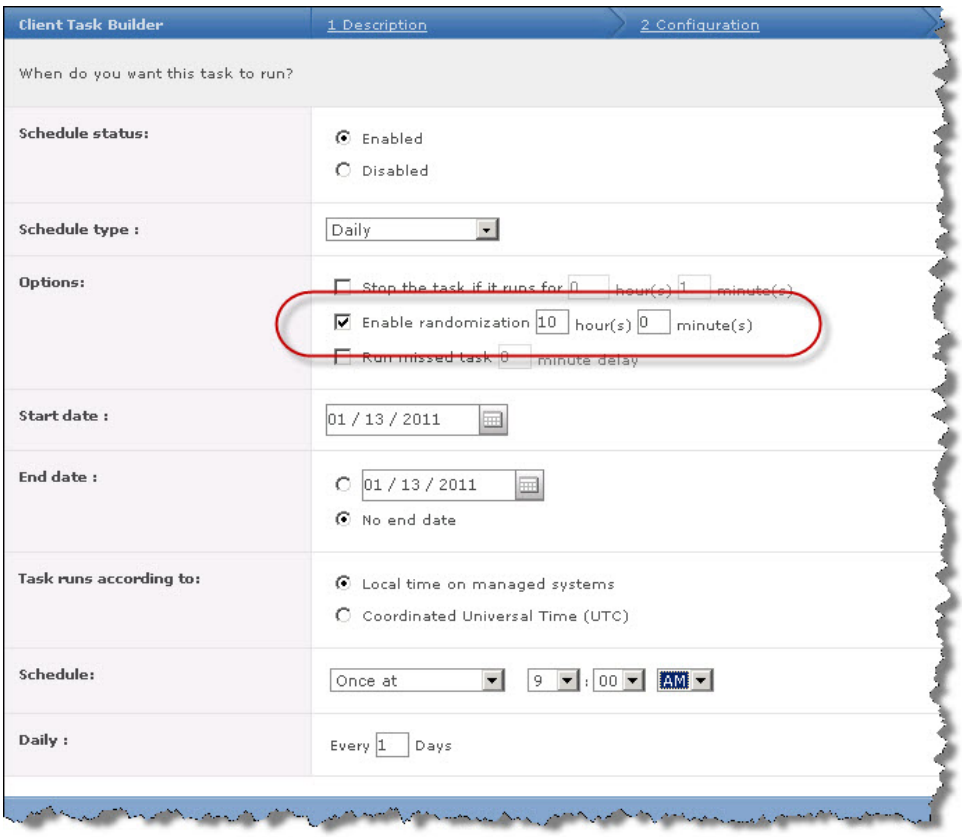
The last and most important step in configuring your client task is to schedule the deployment.

The schedule you choose for your client task is critical because it affects:

- Bandwidth
- Which machines have the latest content for protection
- The quality of your compliance reports

If a deployment task is being deployed to multiple point-products for the first time, you want to gradually roll out the products to some targeted test machines. The schedule you configure depends on the bandwidth available in your environment. For example, if you are upgrading from VirusScan Enterprise 8.7 to 8.8, you can look at the VirusScan Enterprise 8.8 package that you checked into the ePolicy Orchestrator repository and see it is 36 MB. That means each machine you target for deployment is pulling 36 MB from its nearest repository. If your McAfee ePO server is managing 5,000

nodes and you only have one repository, those 5,000 nodes are pulling a total of 180 GB of data from that one repository when the deployment task is executed. To keep that repository from being overwhelmed, you must randomize your deployment.



Many customers forget to enable randomization on their tasks and choose a specific time for their task to run such as noon on a daily basis. If you haven't configured randomization and you deploy a product or signature update at noon on a daily basis, this generates a significant spike in traffic to your repositories at that exact time. This could impact network performance.

Randomization is critical to any client task that uses bandwidth. Always calculate how much bandwidth the deployment needs by taking the size of the deployment package, multiplied by the number of nodes targeted, divided by the number of repositories used. For example, VirusScan 8.8, which is 36 MB, deployed to 1,000 nodes, pulled across 3 repositories, equals 36 GB of data. That 36 GB of data is being pulled across three repositories which equals 12 GB per repository.

36 MB (VSE) * 1,000 (nodes) = 36 GB (total) / 3 (repositories) = 12 GB per repository

The following formula calculates the bandwidth needed to move the 12 GB of data per repository randomly over a 9-hour workday. The total equals 1.33 GB of data per hour pulled from each repository.

12 GB (per repository) / 9 (hours) = 1.33 GB per hour

Updating products

Product updates use the agent to update content such as VirusScan Enterprise DAT files, engines, or product patches.

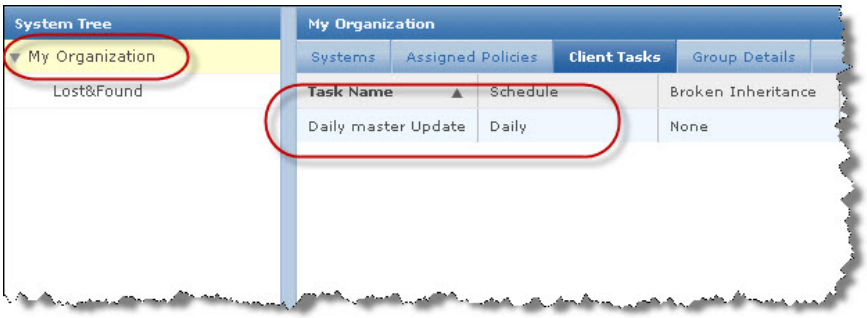
Signatures, or DAT files, are released on a daily basis at approximately 11 a.m. Eastern time and average 200 Kb per day. Optionally, you can deploy other items, such as product patches, to more targeted groups for testing before making them part of your master update task at the My Organization level. When possible, always set product update tasks at the My Organization level, which is the highest level, in the System Tree.

Create a Daily Master Update at the My Organization level.

Task

For option definitions, click **?** in the interface.

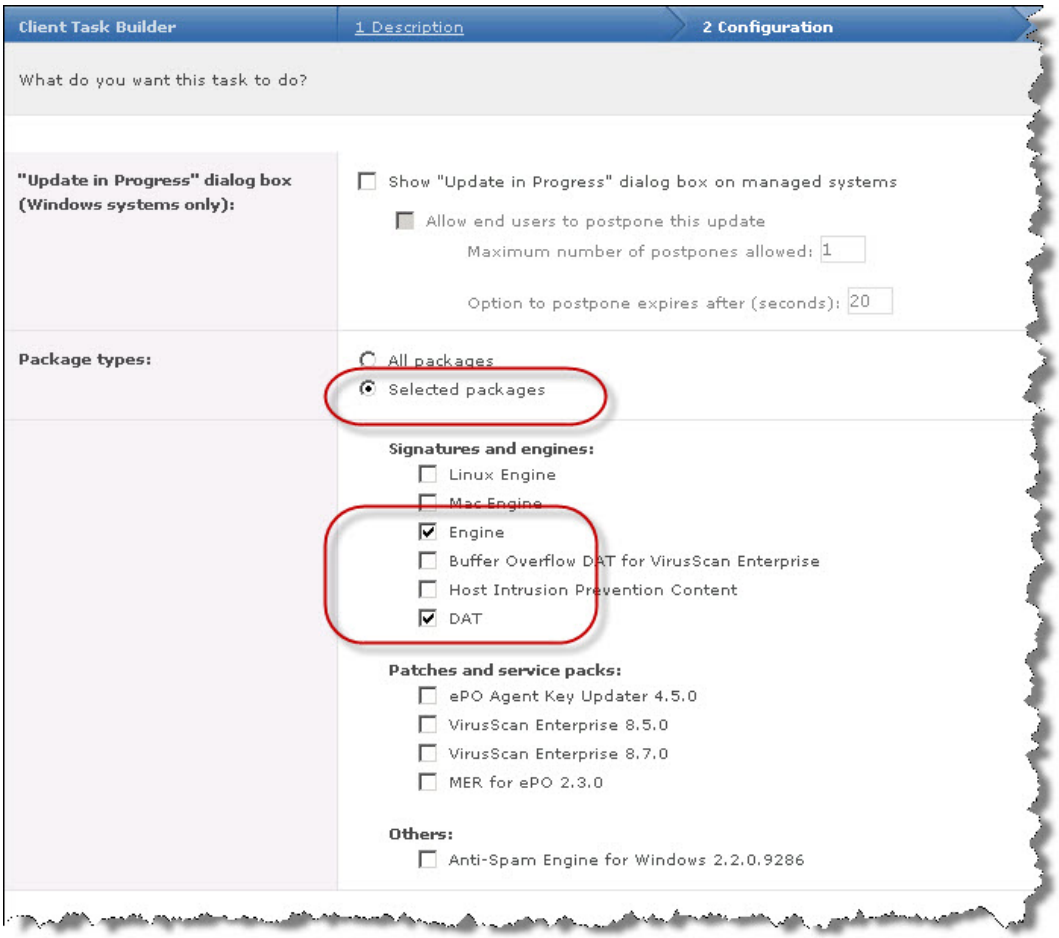
1 Click **Menu | Systems | System Tree** and click **My Organization** in the System Tree pane.



2 From the **Client Tasks** tab, click **Actions | New Tasks** and the Client Task Builder dialog box appears.

3 Type a name, for example `Daily Master Updates`, click **Product Update** from the Type list, and click **Next**. The Client Task Builder dialog box appears.

4 Choose the content to update using this task.



In this example the Daily Master Update task downloads the VirusScan Enterprise DAT and Engine files.

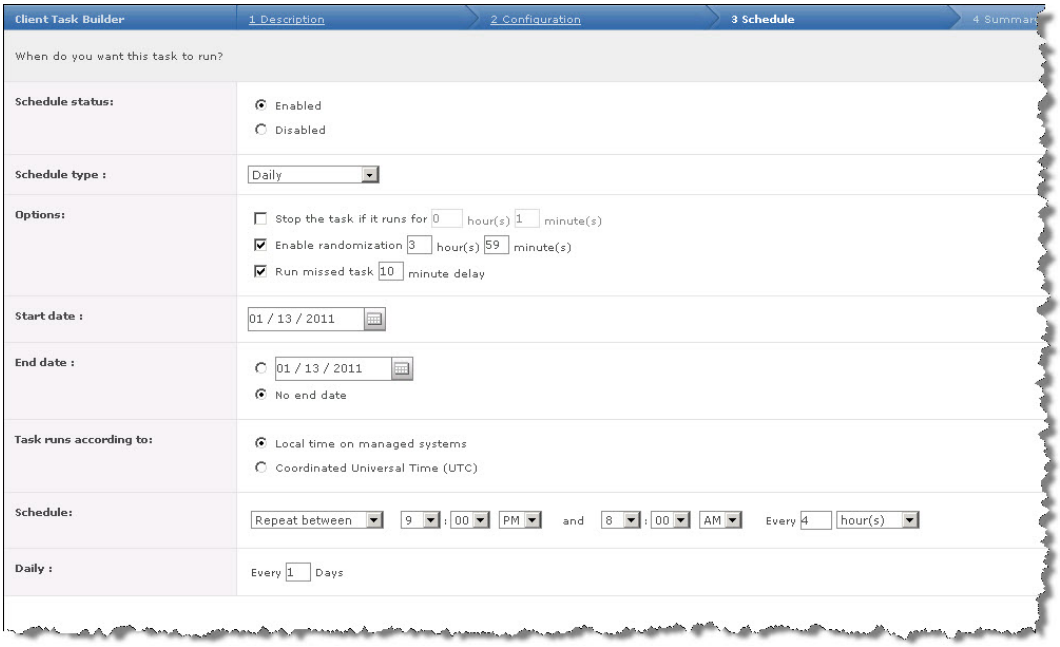
If you would like to deploy a product patch, make a separate client task designed to deploy that patch only. That makes it easier to keep track of your client tasks

5 Click **Next** to configure the schedule for this task.

The key to a good update task is updating several times per day at completely random intervals. Many users think since McAfee releases its signatures once per day then configure the clients to only look for updates once per day. A client can check for updates several times per day at the nearest repository without any negative impact to bandwidth or the repositories. If no update is available the client simply checks again at its next scheduled interval. The network impact is small since the client is looking for a tiny file that is less than 1 KB during each check. This little files tells the client if any new files are available.

The following example starts the task at 9 a.m. and is randomized for 3 hours and 59 minutes. This makes all clients check their nearest repository from 9 a.m. to 12:59 p.m. for the selected content. This process starts again at 1 p.m. since the task is configured to run every 4 hours. This continues for 23 hours, which is 8 a.m. the next morning and starts all over again the next day at 9 a.m. This example updates six times per day at completely random times throughout the day. Also, if the user is away for several days or weeks their computer executes this task 10 minutes after it is turned on.

You can reduce or increase how often your clients check for updates depending on your organization's policy. For example, you can have the task run every 6 hours which means clients are updating only 4 times per day. The most important thing to remember is make your randomization window as large as possible. If you are updating every 6 hours then configure your randomization for 5 hours 59 minutes.



Many users fail to take advantage of the maximum randomization window. They might be updating every 6 hours but randomization is set for only 15 minutes. This means if the task is starting at 9 a.m. the clients will be updating from 9:00 a.m. to 9:15 a.m. If you have 10,000 nodes running this task, they are all checking their repositories in that 15 minute window. Those repository connections significantly impacting network bandwidth. Always randomize your task as much as the window you have chosen allows.

6

10 Server tasks

Server tasks are any item that is scheduled to run on the McAfee ePO server itself. Using server tasks properly can significantly improve efficiency in your organization.

Server tasks automate many of the common items you performed on a daily or weekly basis manually. Server tasks are automatically added as new extensions are added to ePolicy Orchestrator. For example, encryption related server tasks appear when the encryption extension is installed. This means ePolicy Orchestrator is configured around the components you actually manage instead of having options for products you never use. Some common server tasks include:

- Performing an action using the results of a query
- Emailing and exporting reports automatically on a regular basis
- Pulling and replicating content automatically from the McAfee site
- Purging older events automatically from the McAfee ePO server database
- Deleting inactive machines automatically from your system Tree

Contents

- *Perform an action on a query*
- *Creating an automatic report email or export*
- *Create an automatic content pull and replication*
- *Purge events automatically*
- *Purging events by query*
- *Deleting inactive systems automatically*

Perform an action on a query

Server tasks allow you to automate activities on the McAfee ePO server by performing an action using the results of a query on a scheduled basis.

This process requires you to:

1 Give your server task a descriptive name.

2 Choose an action then a subaction. This is the most important part of creating your task. After the task performs the first action it performs the subaction based on the results of the original action. For example:

- Run a query on the machines that have not communicated with the McAfee ePO server in over 30 days.
- Email that report to a specific administrator.
- Optionally, you can delete those machines from your System Tree after the report has been sent.

Another example:

- Create a query (or use a preconfigured query) and return all machines that have had a virus in the past 12 hours.

  You can limit the query to a specific area in your System Tree, for example the New York data center.

- Export that report into HTML.
- Send the link to the help desk, for example in the New York data center, so they can view it on their help-desk portal.
- Optionally, you can apply a tag to machines that have returned those viruses within the specific time-frame, then launch an on-demand scan on those troubled machines based on the tag. There are dozens of options you can use to take actions on a specific query. See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details. The main requirement is that your query must return a table of managed systems, so ePolicy Orchestrator can take action on those systems.

Creating a server task

Create a server task.

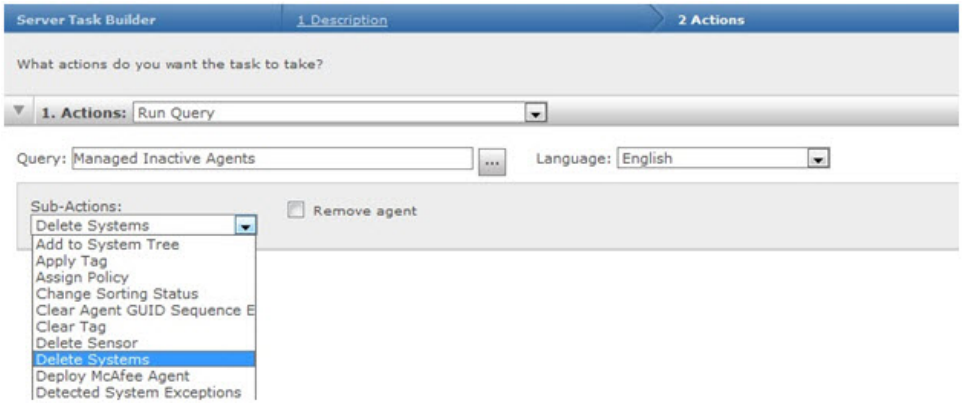
Task

For option definitions, click **?** in the interface.

1 Click **Menu | Automation | Server Tasks** and click **Actions | New Task**. The Server Task dialog box appears.

2 Give the task a name, for example `Manage Inactive Systems`, and click **Next**. The Actions dialog box appears.

3 Configure a weekly report.
   - Click **Run Query** from the Actions list.
   - Click **Managed Inactive Agents** query from the Query list dialog box that appears, then click **OK**.
   - Create a subaction that deletes the inactive agents generated by the report, then click **Next**



   Notice you chose an action then a subaction. This allows the task to perform the first action then it performs the subaction based on the results of the original action.

4 Schedule the server task to run. For example, on a busy McAfee ePO server make sure you run this task during off hours, either nightly or weekly.

Creating an automatic report email or export

Emailing and exporting reports is a very powerful feature of server tasks. You can use custom or preconfigured queries, run them, and email the reports generated to anyone.

ePolicy Orchestrator offers very powerful dashboards but it might not be feasible for certain groups in your organization to log into ePolicy Orchestrator and monitor these dashboards. For example, you might want the help desk to view ePolicy Orchestrator dashboards but there are too many users on the help desk team. Emailing reports is an alternative to dashboards and you can export reports to a folder in HTML. This allows you to copy reports to an existing help-desk portal. The benefits of automating reports include:

- Scheduling reports reduces the load on a busy McAfee ePO server.
- Reports can be sent to an easily maintained email distribution list.
- Mobile administrators can receive emailed reports without direct access to the McAfee ePO server.
- Auditors can receive emailed reports without direct access to the McAfee ePO server.

Create an email report.

Task

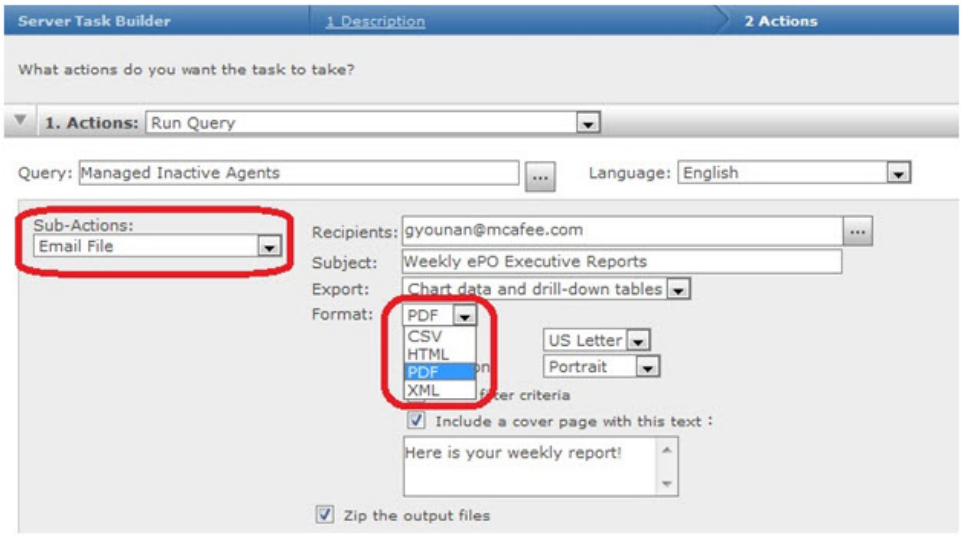
For option definitions, click **?** in the interface.

1 Click **Menu | Automation | Server Tasks**, and click **Actions | New Task**. The Server Task dialog box appears.

2 Give the task a name, for example `Manage Inactive Systems` and click **Next**. The Actions dialog box appears.

3 Configure an email report.

- Click **Run Query** from the Actions list.
- Click **Managed Inactive Agents** query from the Query list dialog that appears, then click **OK**.
- Create a subaction that emails the file as a PDF file to your selected recipients, then click **Next**.



- Choose the custom or preconfigured query that you want to email and enter the email address where you want the email sent. Choose the format you would like for the reports. Optionally, you can zip your files to reduce their size.

> You can chain additional Actions under one task by using the plus sign on the far right of the server task. This lets you send multiple queries under one server task instead of having to build multiple server tasks.

4 Schedule when the server task should run. For example, on a busy ePO server make sure you run this task during off hours, either nightly or weekly.

Create an automatic content pull and replication

One of the most important functions that your McAfee ePO server performs daily is pulling content from the public McAfee servers. This keeps your protection signatures up to date for McAfee products like VirusScan Enterprise and Host Intrusion Prevention System.

The primary steps are:

1 Pull content from McAfee into your master repository, which is always the McAfee ePO server.

2 Replicate that content to your distributed repositories. This ensures multiple copies of the content is available and remains synchronized. This allows clients to update their content from their nearest repository.

The most important content is the DAT files for VirusScan Enterprise released daily at approximately 11 a.m. Eastern Time.

Optionally, many users with larger environments choose to test their DAT files in their environment before deployment to all their machines. To do this use the different branches offered in the repositories. These branches, Evaluation, Previous, and Current, allow you to place different versions

of content into each branch. Then the different versions can be rolled out to a selected group of test machines before a full deployment to the entire environment. See Validating DAT and Other Content with ePO 4.5 PDF document on the KnowledgeBase.

Disabling master repository client pulls

To improve the McAfee ePO server performance, if you have distributed repositories, you might need to disable master repository client pulls.

Many customers perform their pull task earlier in the day, for example 1 p.m. but they do not replicate their repositories until later in the evening, for example 7 p.m. They mistakenly think they are reducing replication bandwidth by replicating during off hours instead of critical business hours. This can actually cause problems.

If the master repository pulls new content there is a version timestamp that informs the agents that the master repository is up to date but the distributed repositories are now out of date. This causes the agents to go to the master repository, no matter how far away it might be, as one of their update locations, and they ignore their local, nearby repository since it does not have the latest content. This can have a negative bandwidth impact during business hours. Just the opposite of the original goal.

To avoid this problem:

- Disable the master repository as an update option (described below) so that your agents are not allowed to pull any content from the master repository. Instead they are forced to wait until the distributed repositories receive the latest content during replication.
- When you perform your pull to the master repository immediately follow the pull with a replication to your distributed repositories.
- Wait until the evening to do your pull and replication if replication bandwidth use is a concern during business hours.

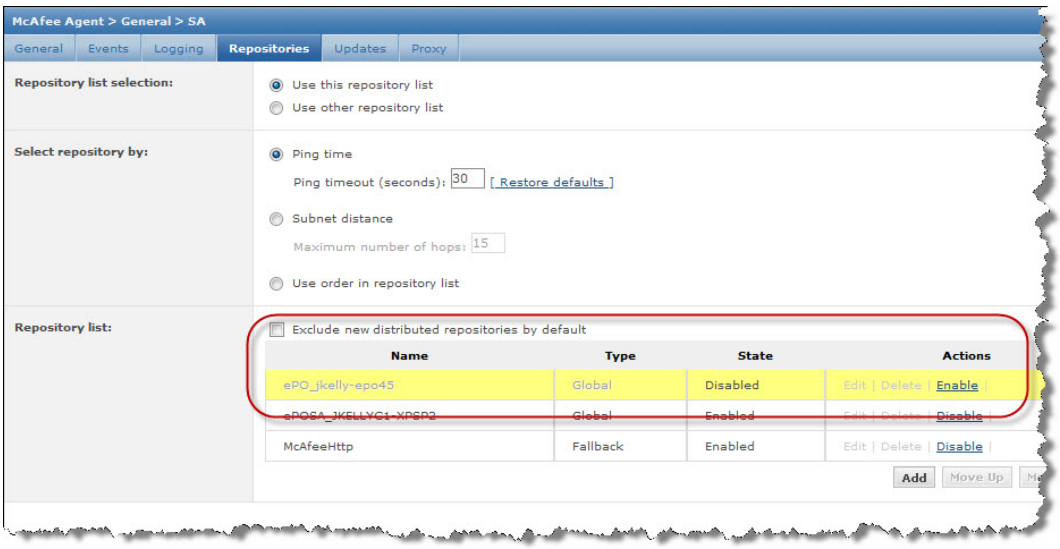
Disable master repository client pulls if you have distributed repositories.

Task

1 Open the Policy Catalog, select **McAfee Agents** from the Product list, then select **General** from the Category list.

2 Click **Edit Setting** and the **Repositories** tab.

3 From the Repositories list, find the McAfee ePO server and click **Disable** in the Actions column.



4 Click **Save** to disable the McAfee ePO server repository.

Purge events automatically

Every day hundreds or thousands of events are sent to your McAfee ePO server for processing from all your agents. These events can impact the performance of the McAfee ePO server and SQL Servers.

These events can be anything from a threat being detected, to an update completing successfully. In smaller environments with a few hundred nodes you can purge these events on a nightly basis. But in large environments with thousands of nodes reporting to your McAfee ePO server it is critical to delete these events as they become old.

You need to determine your data retention rate. This can be from one month to an entire year. The retention rate for most organizations is about six months. For example, as your events get six months old, on schedule, they are deleted from your database.

It is very important that you purge your database on a nightly basis of events that have become stale. In large environments your database size directly impacts the performance of your McAfee ePO server and you must have a clean database.

ePolicy Orchestrator does not come with a preconfigured Server Task to purge task events. This means many users never create a task to purge these events and over time the McAfee ePO server SQL database starts growing exponentially and is never cleaned.

There are two important event types in your database; client events and threat events. These two event types are the bulk of your event data in your database. To find out the total number of client and threat events in your database see *Reporting*.

Creating a purge events by query server task

Create an automated server task to delete all events in the database that are older than *X* number of days (where *X* days is the retention rate for your organization).

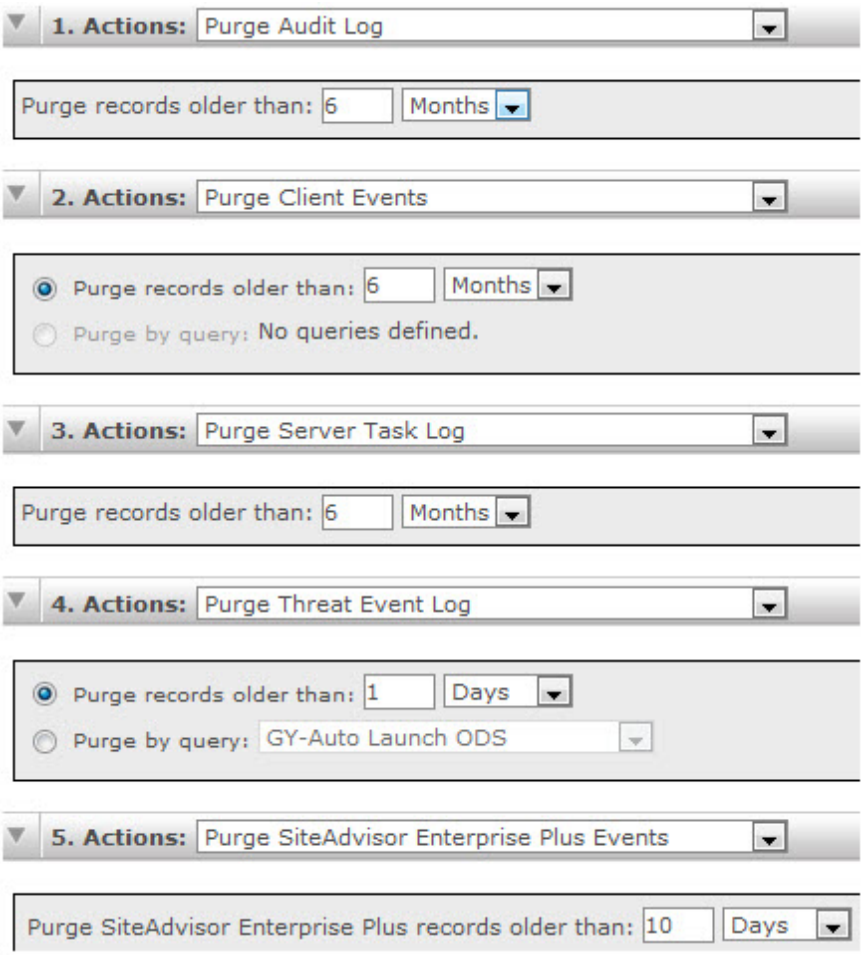
Task

For option definitions, click **?** in the interface.

1 Click **Menu | Automation | Server Tasks**, then click **Action | New Task**. The Server Task Builder dialog box appears.

2 Give the task a name, for example `Delete client events`, and from the Actions tab configure the following from the Actions list:

- **Purge Audit Log** — Purge after 6 months.
- **Purge Client Events** — Purge after 6 months.
- **Purge Server Task Log** — Purge after 6 months.
- **Purge Threat Event Log** — Purge after day.
- **Purge SiteAdvisor Enterprise Plus Events** — Purge after 10 days.


1. Actions: Purge Audit Log
Purge records older than: 6 Months
2. Actions: Purge Client Events
Purge records older than: 6 Months
Purge by query: No queries defined.
3. Actions: Purge Server Task Log
Purge records older than: 6 Months
4. Actions: Purge Threat Event Log
Purge records older than: 1 Days
Purge by query: GY-Auto Launch ODS
5. Actions: Purge SiteAdvisor Enterprise Plus Events
Purge SiteAdvisor Enterprise Plus records older than: 10 Days

You can chain the actions all in one task so you don't have to create multiple tasks.

This example has a purge for SiteAdvisor Events because SiteAdvisor events are not included in the normal events table, therefore it requires its own purge task. The retention for SiteAdvisor

events is only 10 days because it collects all URLs that are visited by managed machines. This can save a lot of data in environments with greater than 10,000 nodes. Therefore this data is saved for a much shorter time compared to other event types.

3 Schedule the task to run every day during non-business hours, then click **Save**.

Purging events by query

You can use a custom configured query as a base to clear client events.

There are several reasons why you might need to purge data or events based on a query. For example, there could be a high number of a specific events overwhelming your database. In this example you might not want to wait for the event to age out if you are keeping your events for six months, and you would like that specific event deleted immediately or nightly.

Configure purging data based on the results of a query.

Task

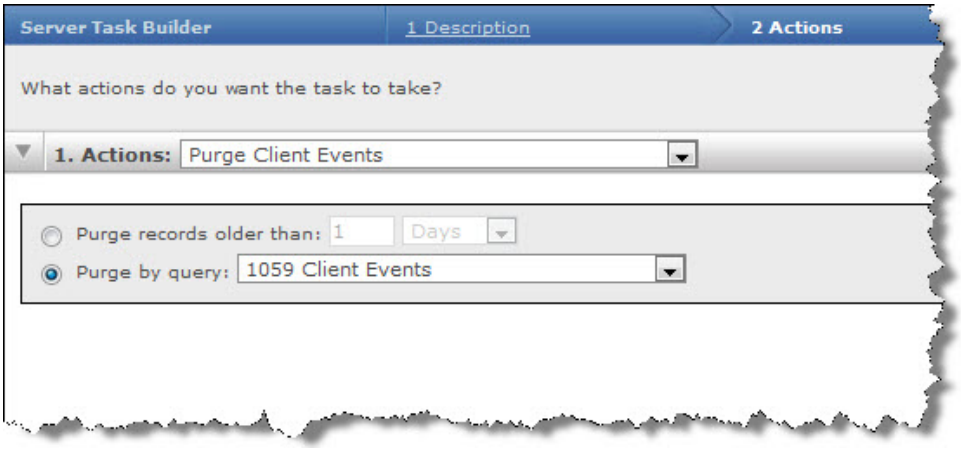
For option definitions, click **?** in the interface.

1 Configure a query to return the events you want purged. See *Creating custom event queries* for details.

2 Click **Menu | Automation | Server Tasks**, then click **Action | New Task**. The Server Task Builder dialog box appears.

3 Give the task a name, for example `Delete 1059 client events`, and from the **Actions** tab, click **Purge Client Events** from the Actions list.

4 Click **Purge by Query** and select the custom query you created in step 1.



This menu is automatically populated when table queries are created for client events.

5 Schedule the task to run everyday during non-business hours, then click **Save**.

Deleting inactive systems automatically

Most environments are constantly changing, new systems are added and old systems removed. This creates inactive McAfee Agent systems that, if not deleted, can ultimately skew your compliance reports.

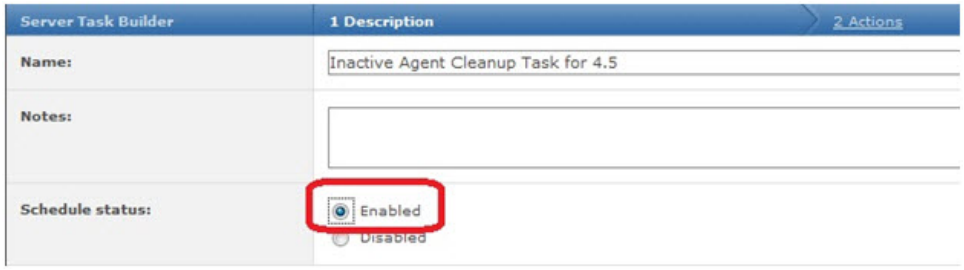
As systems are decommissioned, or disappear because of extended travel, users on leave, or other reasons, remove them from the System Tree. Removing these systems ensures the reports you run are returning data on systems that have recently communicated with the McAfee ePO server, not outdated systems that have not communicated in weeks. An example of a skewed report might be your DAT report on compliance. If you have systems in your System Tree that have not reported into the McAfee ePO server for 20 days then they appear as out of date by 20 days and ultimately skew your compliance reports.

You can of course create a query and report to filter out systems that have not communicated with the McAfee ePO server in X number of days but it is more efficient to either delete or automatically move these systems. Most organizations choose a number between 14 and 30 days of no communication to delete or move systems. For example, if a system has not communicated with the McAfee ePO server you can delete or move that system to a group in your tree that you can designate as *Inactive Agents*. There is already a preconfigured task that is disabled by default that you can edit and enable on your server.

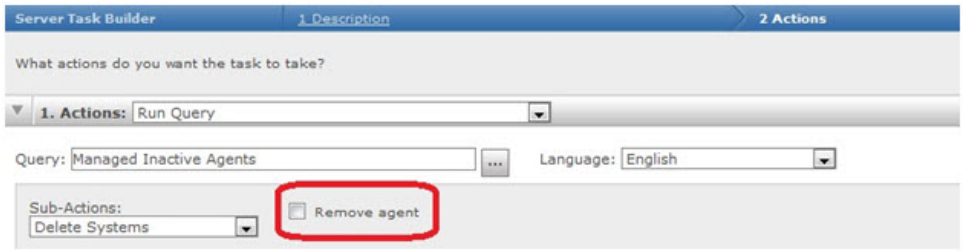
Edit and enable the Inactive Agent Cleanup server task.

1 Click **Menu | Automation | Server Tasks** and click **Edit** for the Inactive Agent Cleanup Task for 4.5 in the Action column. The Server Task dialog box appears.

2 If needed, change the name, click **Enabled** next to Schedule status, and click **Next**. The Actions dialog box appears.



You can see this server task uses an action on the results of a query called Managed Inactive Agents and whatever systems are returned from that query are deleted according to the subaction.



See *Changing the Managed Inactive Agents query* for details.

Do **not** click the checkbox to Remove agent.

The Remove agent setting causes ePolicy Orchestrator to delete the McAfee Agent from the inactive systems when they are removed from the System Tree. Without the agent installed, when the removed system reconnects to the network it cannot automatically start communicating with the McAfee ePO server and reinserts itself back into the System Tree.

3 Optional. Instead of using the default subaction Delete Systems, you can select Move Systems to another Group. This moves the systems found by the query to a designated group in your System Tree in case you want to investigate these systems further.

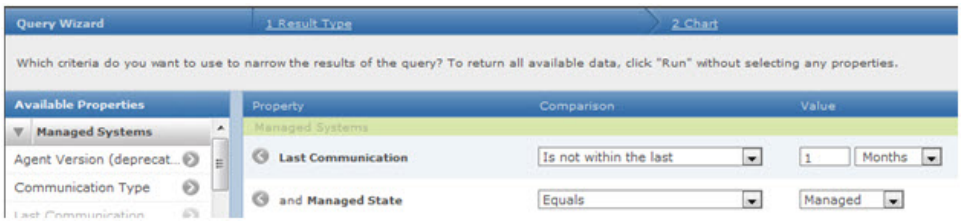
You might be concerned about deleting systems out of your System Tree because you think that the system will never report back to the McAfee ePO server if it returns to the network. This is not the case. Deleting a system from the tree only deletes the record for that system from the ePolicy Orchestrator database. If the system physically exists it will continue to perform normally with the last policies it received from the McAfee ePO server for its applicable products.

4 Click **Next**, schedule when you want this server task to run and save the server task.

Changing the Managed Inactive Agents query

The Inactive Agent Cleanup server task uses a preconfigured query named Managed Inactive Agents. Whichever systems are returned from the query are deleted or moved according to the subaction configured in the server task.

If you want to see what that query is using as a filter, edit that specific query in the query area. In the following figure, the query has only two simple filters and only returns agents that have not communicated with the McAfee ePO server in over a month. You can edit the query and adjust the number of days for the last communication to change the actions of the server task.



See *McAfee ePolicy Orchestrator 4.5 Product Guide* for details about working with queries.

11 Reporting

ePolicy Orchestrator ships with its own querying and reporting capabilities. These are highly customizable, flexible and easy to use. The **Query Builder** and **Report Builder** creates and runs queries and reports that result in user-configured data in user-configured charts and tables. The data for these queries and reports can be obtained from any registered internal or external database in your ePolicy Orchestrator system.

Contents

- *Reporting overview*
- *Custom queries*

Reporting overview

The ePolicy Orchestrator 4.5 server includes a powerful and simple to use query system. You can use the preconfigured queries, create custom queries, and use the output of the queries to perform tasks. For example to create reports, or delete inactive nodes.

Creating reports with previous versions of ePolicy Orchestrator required extensive knowledge of SQL statements and Crystal Reports. The new ePolicy Orchestrator 4.5 query system allows you to create custom reports configuring these four basic items:

- **Result Type** — Identifies what type of data the query retrieves, and determines the available selections in the rest of the wizard.
- **Chart Type** — Specifies the type of chart or table to display the data it retrieves.
- **Columns** — Selects the data to display. If you select Table, this configures the table. If you select a type of chart, this configures the drill-down table.
- **Filter** — Specifies displayed criteria by selecting properties and operators to limit the data retrieved by the query.

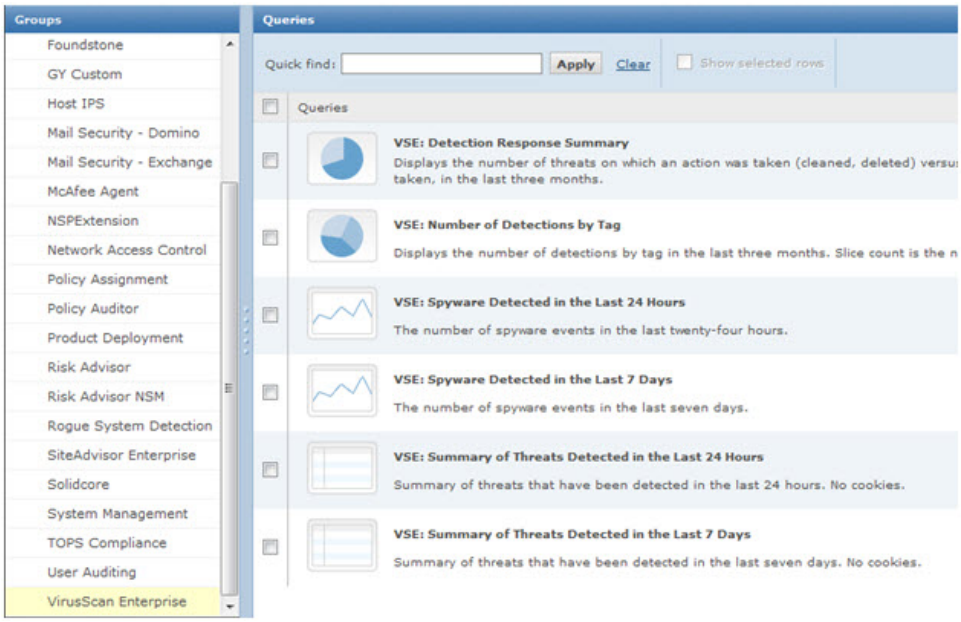
To view one of the preconfigured queries, click **Run** and the query output appears. You can then:

- Save the output as a report
- Duplicate the query and change the output
- Click any results you see in the query system for additional information
- Take action on certain results as you normally would in the System Tree

As you add new products using extensions to The McAfee ePO server new preconfigured queries and reports become available.

See *McAfee ePolicy Orchestrator 4.5 Product Guide* and *McAfee ePolicy Orchestrator 4.5 Reporting Guide* for details.

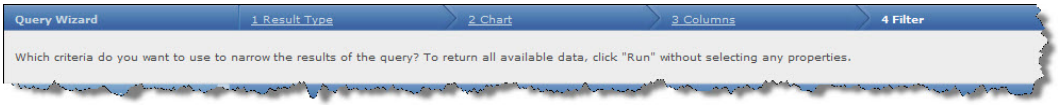
The following example shows some of the categories of preconfigured queries provided with the ePolicy Orchestrator software.


Groups
Foundstone
GY Custom
Host IPS
Mail Security - Domino
Mail Security - Exchange
McAfee Agent
NSPExtension
Network Access Control
Policy Assignment
Policy Auditor
Product Deployment
Risk Advisor
Risk Advisor NSM
Rogue System Detection
SiteAdvisor Enterprise
Solidcore
System Management
TOPS Compliance
User Auditing
VirusScan Enterprise
Queries
Quick find:
Apply
Clear
Show selected rows
Queries
VSE: Detection Response Summary
Displays the number of threats on which an action was taken (cleaned, deleted) versu
taken, in the last three months.
VSE: Number of Detections by Tag
Displays the number of detections by tag in the last three months. Slice count is the n
VSE: Spyware Detected in the Last 24 Hours
The number of spyware events in the last twenty-four hours.
VSE: Spyware Detected in the Last 7 Days
The number of spyware events in the last seven days.
VSE: Summary of Threats Detected in the Last 24 Hours
Summary of threats that have been detected in the last 24 hours. No cookies.
VSE: Summary of Threats Detected in the Last 7 Days
Summary of threats that have been detected in the last seven days. No cookies.

Custom queries

Creating custom queries is a straightforward process on the McAfee ePO server, plus you can duplicate and modify existing queries to change the output and reports.

Custom queries can be created in four simple steps. Like most tasks in ePolicy Orchestrator you can follow the simple wizard at the top of the screen.


Query Wizard
1 Result Type
2 Chart
3 Columns
4 Filter
Which criteria do you want to use to narrow the results of the query? To return all available data, click "Run" without selecting any properties.

There are two ways to approach custom queries:

- You can determine exactly what kind of query you want to create before you attempt to create it.
- You can explore the query wizard and try different variables to see what kind of queries can be made.

Both approaches are valid and can yield interesting data about your environment. If you are new to the query system, try exploring different variables to get more familiar with the kind of data that ePolicy Orchestrator returns.

Once you have built your report, you can take action on the results if the data returned is for managed systems. This means you can do anything you could do in the System Tree. For example, wake-up machines, update them, delete them, or move them to another group. This is very useful when running reports on machines that:

- Have not communicated with the McAfee ePO server in a while
- Are suspected of not working properly when you attempt to wake them up
- Need a new agent deployed to them directly from the McAfee ePO server

Creating custom event queries

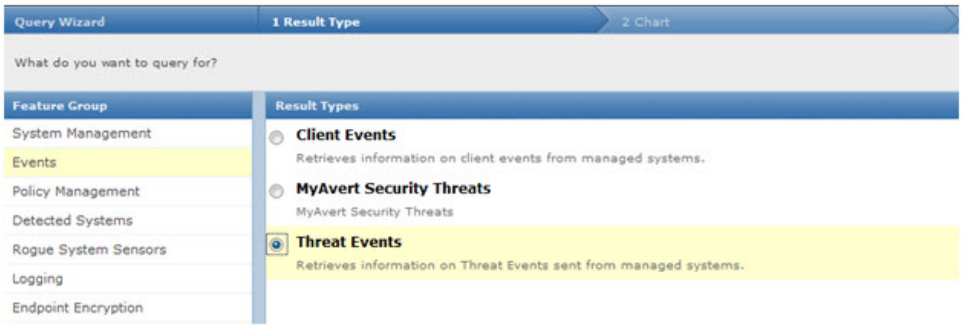
Create a custom query.

Task

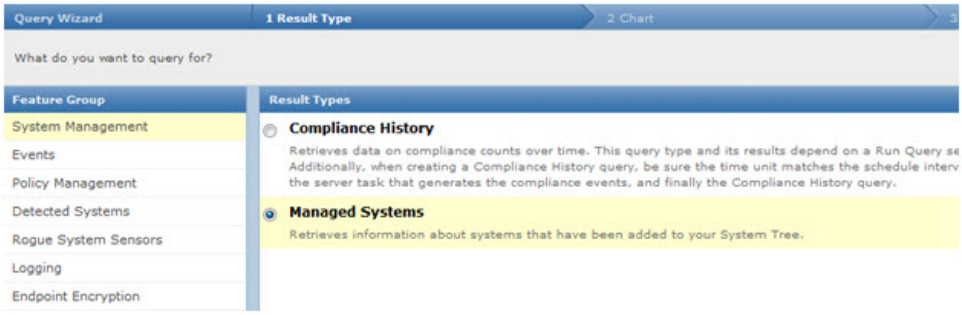
1 Click **Menu | Reporting | Queries**, then **Actions | New Query**. The Query Wizard appears starting with the Result Types tab.

The result types are organized into groups on the left hand side of the page. Depending on what extensions have been checked into ePolicy Orchestrator these groups vary. Most of the result types are self explanatory but two of the more powerful result types are Threat Events and Managed Systems. You can access these two events types as shown in the following examples.

- **Threat Events** — In the following, click **Systems Events** in the Feature Group and **Threat Events** in the Result Type.

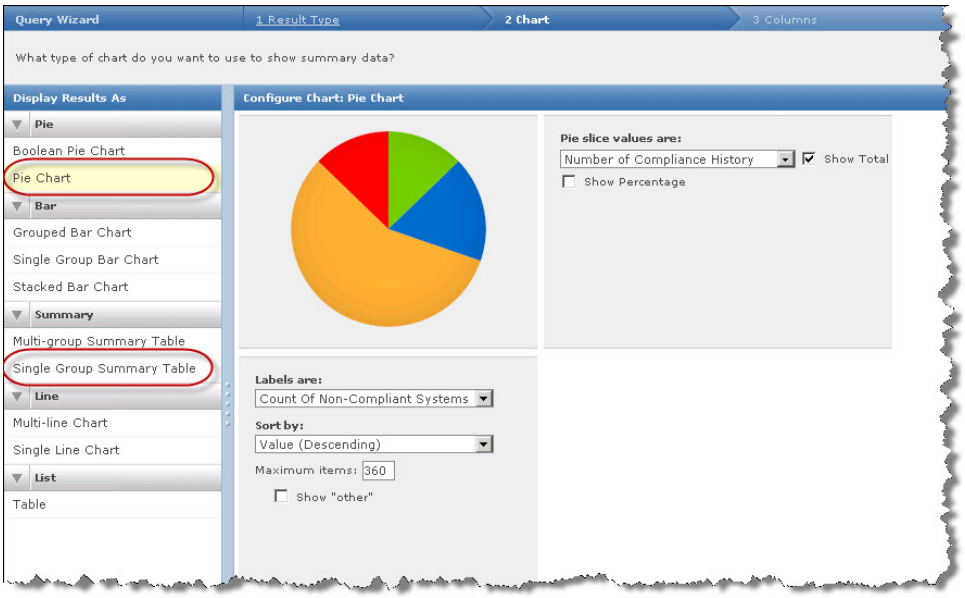


- **Managed Systems** — In the following, click **Systems Management** in the Feature Group and **Managed Systems** in the Result Type.


Query Wizard
1 Result Type
2 Chart
What do you want to query for?
Feature Group
System Management
Events
Policy Management
Detected Systems
Rogue System Sensors
Logging
Endpoint Encryption
Result Types
Compliance History
Retrieves data on compliance counts over time. This query type and its results depend on a Run Query se
Additionally, when creating a Compliance History query, be sure the time unit matches the schedule interv
the server task that generates the compliance events, and finally the Compliance History query.
Managed Systems
Retrieves information about systems that have been added to your System Tree.

2 You must choose your chart type. There are several chart types to choose from and some are more complex than others. The two simplest charts are the pie chart and the single group summary table. The pie chart is good for comparing multiple values in a graphic format and the summary table is good for viewing a data set with over 20 results.

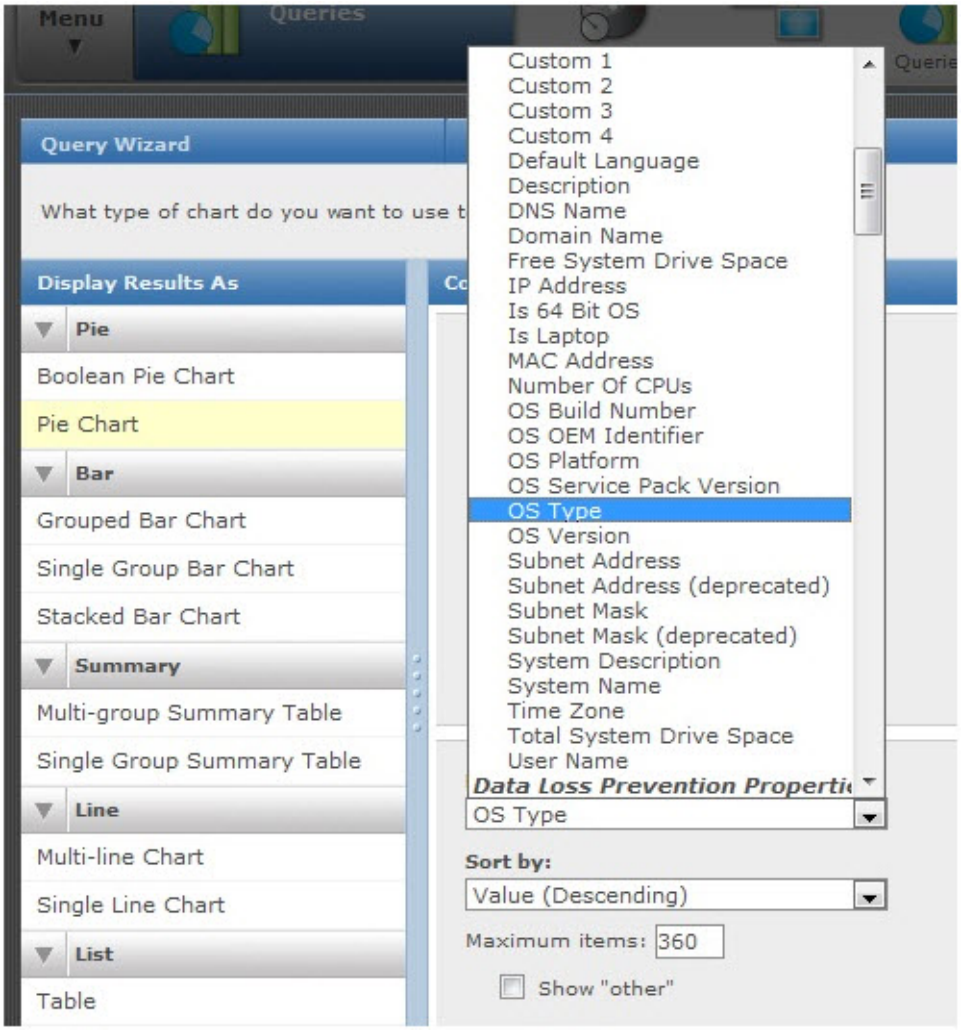
Click **Pie Chart** under Display Results Type.


Query Wizard
1 Result Type
2 Chart
3 Columns
What type of chart do you want to use to show summary data?
Display Results As
Pie
Boolean Pie Chart
Pie Chart
Bar
Grouped Bar Chart
Single Group Bar Chart
Stacked Bar Chart
Summary
Multi-group Summary Table
Single Group Summary Table
Line
Multi-line Chart
Single Line Chart
List
Table
Configure Chart: Pie Chart
Pie slice values are:
Number of Compliance History
Show Total
Show Percentage
Labels are:
Count Of Non-Compliant Systems
Sort by:
Value (Descending)
Maximum items: 360
Show "other"

3 You must choose the label or variable that you want the report to display. There are many variables you can choose to have the McAfee Agent reports display.

Many times the report does not have to return data on McAfee products. For example you can report on the operating system versions used in your environment.

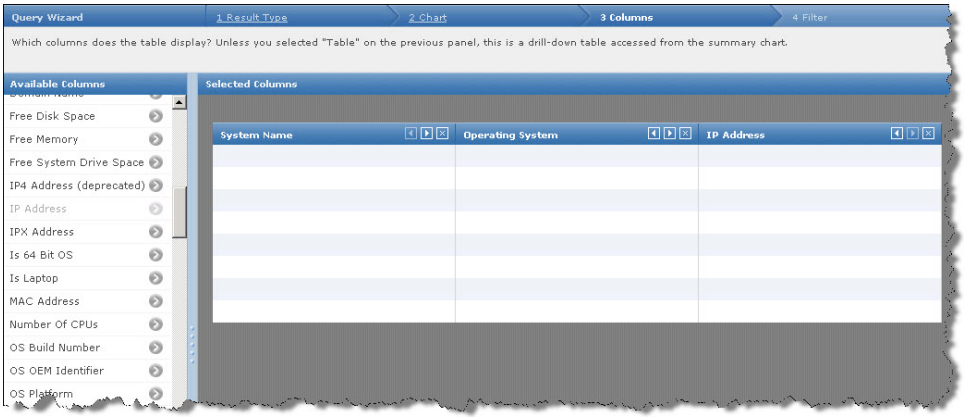
In the **Labels are** list, click **OS Type**.



4 You can choose the columns that you want to see if you drill down on any of the variables in your report. This is not a critical component when building your query and can be adjusted at a later time.

You can also drag and drop your columns from left to right and add and remove columns that you want displayed.

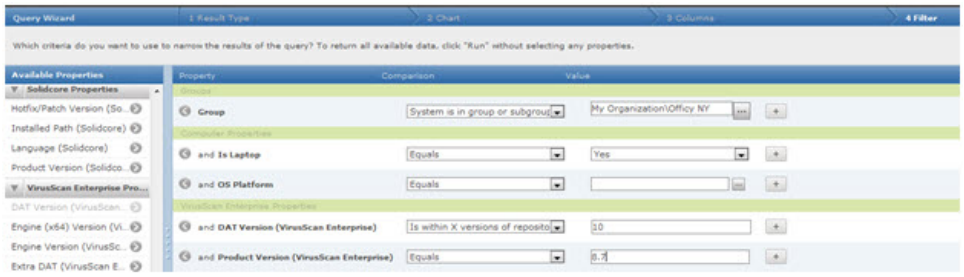
Click **Next** to use the default columns.



You can filter the data that you want the query to return. You can leave the filter area blank which will return every device in your tree or only return results you are interested in. Some options for filtering include choosing:

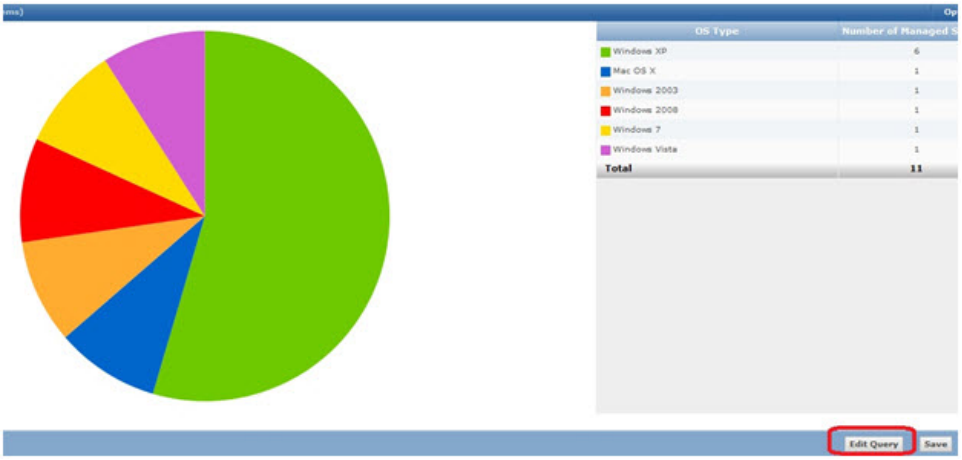
- A group in your system tree where report applies. For example, a geographic location or office.
- To return only machines that are laptops or desktops
- To return only a specific operating system platform. For example, servers or workstations.
- To return only machines that have an older DAT version
- To return only machines that have an older version of VirusScan Enterprise
- To return machines that have only communicated with the McAfee ePO server in the past 14 days

The following example displays configuring some of these filter examples.



5 Click **Next** to not create any filters and display all of the operating system types.

6 Click **Run** to generate the report and see the results.



After you create the reports and display the output you can fine tune your report without starting again from the beginning. To do this, click **Edit Query**. This allows you to go back and adjust your report and run it again within seconds.

When you have made all the changes to your report to save it permanently, click **Save**. Then it is included with your dashboards and you can run it any time.

Event summary queries

There are two important event types in your database, client events and threat events. These two event types make up most of your event data in your database. Determine how many events are stored in your database. This helps you manage any performance problems these events can cause your McAfee ePO server and data base. See *Purging events automatically* for additional information.

Client events from your agents relate their task status to ePolicy Orchestrator. Items like update complete, update failed, deployment completed, or encryption started are considered client events. Threat events include a virus was found, a DLP event was triggered, or an intrusion was detected. Depending on which products you have installed and which events you are collecting there might be thousands or even millions of these events in your database.

ePolicy Orchestrator does not include any pre-configured queries to display which and how many events are in your ePolicy Orchestrator database. But, you can build your own queries to show this data.

Creating client event summary queries

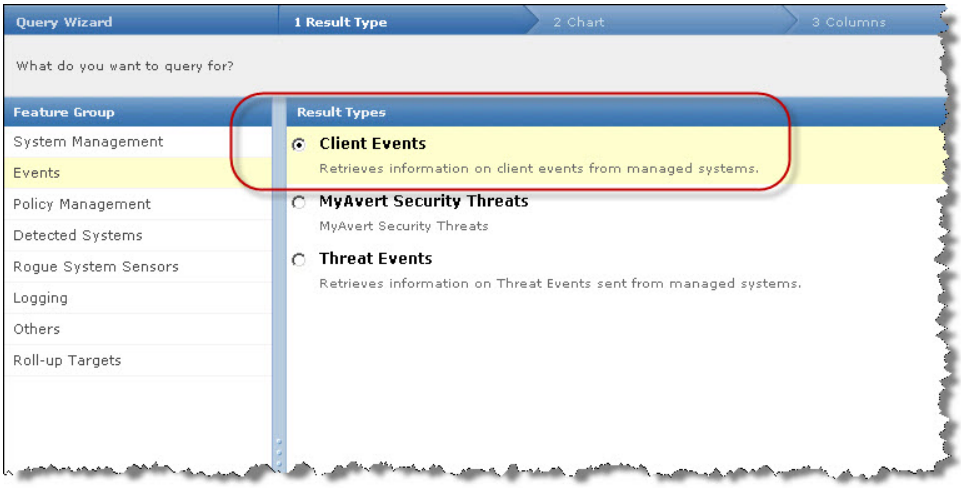
Create a new client events summary query. It displays events sent from your McAfee Agents to ePolicy Orchestrator. Items like update complete, update failed, deployment completed, or encryption started are considered client events.

Task

1 Click **Menu | Reporting | Queries**, the Queries dialog box appears.

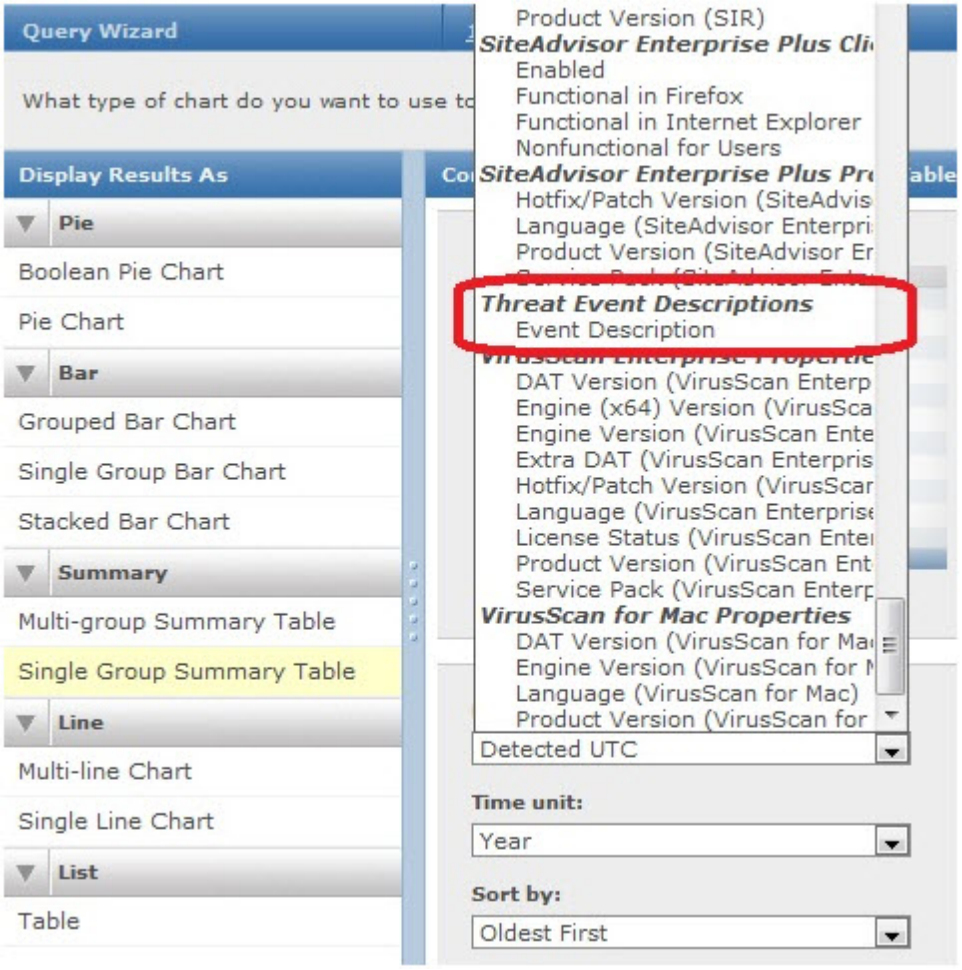
2 Click **Actions | New Query** and the Query Wizard appears starting with the Result Types tab.

3 Click **Events** in the Features Group and **Client Events** in the Result Type. Click **Next** to continue to the Chart dialog box.



4 Under Summary, click **Single Group Summary Table**, to display a total count of all the client events in the events table.

5 Click **Event Description**, in the **Labels are list**, under Threat Event Descriptions to create a filter with a good human readable description of the events.



Optionally, you can also filter on the Event ID which is the number that represents client event data in ePolicy Orchestrator. See *McAfee Point Product generated Event IDs listed in ePO*, KnowledgeBase Article KB54677.

6 If needed, adjust the columns based on what kind of information you want displayed This is not critical for the creation of the query.

7 Click **Next**, the Filter dialog box appears. You do not need any filtering since you want every single client event returned in the database. Optionally, you can create a query based on events generated within a certain time, for example the last 24 hours, or the last 7 days.

8 Click **Run** to display the query report.

GY-All Client Events by Description	
Event Description	**Number of Client Events**
Update Successful	173
Deployment Failed	49
Update Failed	45
Deployment Successful	24
Logon Event	6
System Boot Event	3
Activation Complete Event	1
Activation Start Event	1
Crypt Start Event	1
Crypt Volume Complete Event	1
Crypt Volume Start Event	1
General Exception Event	1
Policy Change Complete Event	1
Policy Change Start Event	1
Total	**308**

In this example there are 308 client events total. If you want, you can click one event and drill down on it to find out more information.

9 Click **Save** and give the report an appropriate name. For example, `All Client Events by Event Description`.

Creating threat events summary query

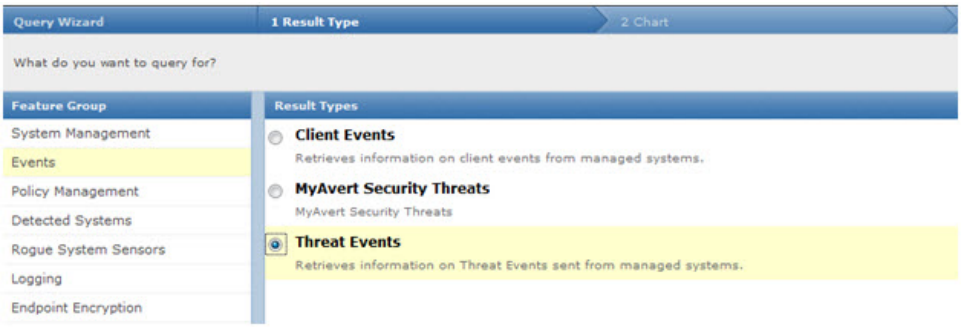
Create a threat events summary query. It displays threat events sent from your McAfee Agents to ePolicy Orchestrator. Threat events include a virus was found, a Data Loss Protection event was triggered, or an intrusion was detected.

Task

1 Click **Menu | Reporting | Queries**, the Queries dialog box appears.

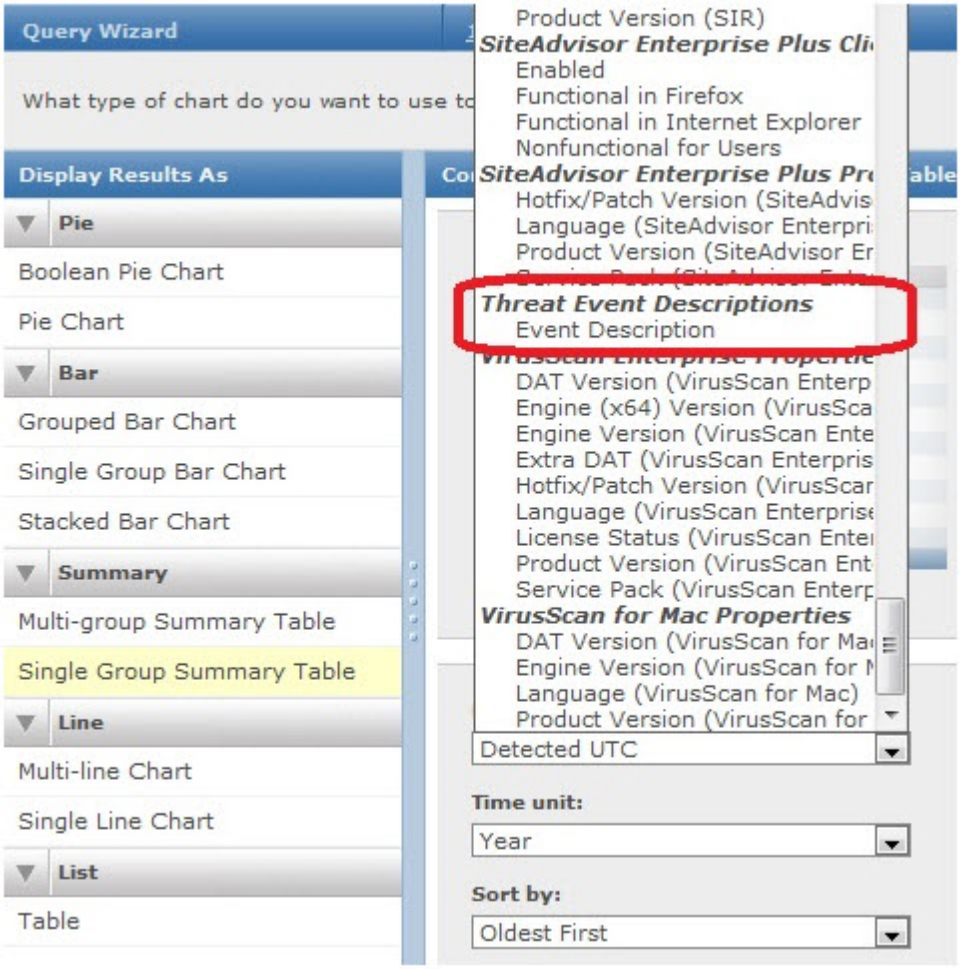
2 Click **Actions | New Query** and the Query Wizard appears starting with the Result Types tab.

3 Click **Events** in the Features Group and **Threat Events** in the Result Type. Click **Next** to continue to the Chart dialog box.



4 Under Summary, click **Single Group Summary Table**, to display a total count of all the client events in the events table.

5 Click **Event Description**, in the **Labels are list**, under Threat Event Descriptions to create a filter with a good human readable description of the events.

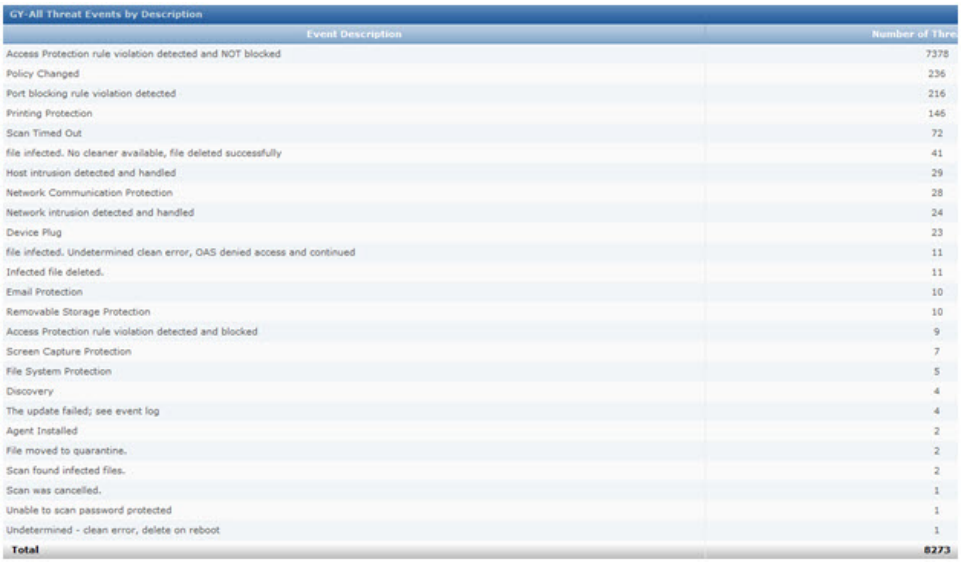


Optionally, you can also filter on the Event ID which is the number that represents client event data in ePolicy Orchestrator. See *McAfee Point Product generated Event IDs listed in ePO*, KnowledgeBase Article KB54677.

6 If needed, adjust the columns based on what kind of information you want displayed. This is not critical for the creation of the query.

7 Click **Next**, the Filter dialog box appears. You do not need any filtering since you want every single client event returned in the database. Optionally, you can create a query based on events generated within a certain time, for example the last 24 hours, or the last 7 days.

8 Click **Run** to display the query report.



GY-All Threat Events by Description

Event Description	Number of Thre
Access Protection rule violation detected and NOT blocked	7378
Policy Changed	236
Port blocking rule violation detected	216
Printing Protection	146
Scan Timed Out	72
file infected. No cleaner available, file deleted successfully	41
Host intrusion detected and handled	29
Network Communication Protection	28
Network intrusion detected and handled	24
Device Plug	23
file infected. Undetermined clean error, OAS denied access and continued	11
Infected file deleted.	11
Email Protection	10
Removable Storage Protection	10
Access Protection rule violation detected and blocked	9
Screen Capture Protection	7
File System Protection	5
Discovery	4
The update failed; see event log	4
Agent Installed	2
File moved to quarantine.	2
Scan found infected files.	2
Scan was cancelled.	1
Unable to scan password protected	1
Undetermined - clean error, delete on reboot	1
Total	**8273**

The McAfee ePO server displays approximately 8,000 threat events total.

The data shown in this example comes from a McAfee ePO server that is only managing a few dozen nodes so these numbers are relatively small. A real production ePolicy Orchestrator database may have millions of threat and client events.

9 To determine approximately how many events you should have on your network use the following formula:

(10,000 nodes) x (1 to 2 million events) = estimated number of events

For example, if you have 50,000 nodes you should be in the range of 5 to 10 million total client and threat events.

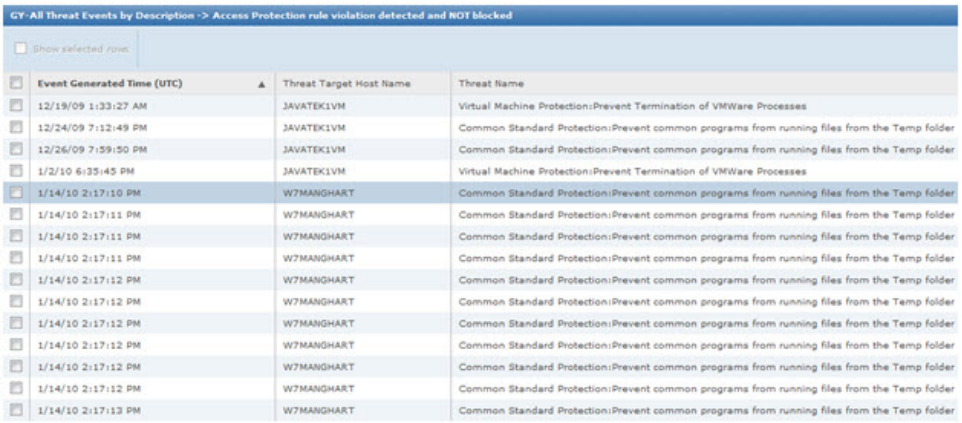
This number will vary greatly based on the number of products and policies you have and your data retention rate. Do not panic if you exceed this number.

If you significantly exceed this number determine why you have so many events. Sometimes this can be normal if you receive a significant number of viruses. This is common in unrestricted networks like universities or college campuses. Another reason for a high event count could be how long you keep the events in your database before purging. Here is what to check:

- Are you purging your events on a regular basis as shown in the *Purging events automatically* section?
- Is there a specific event in the query that is making up a majority of your events?

Remember, it's very common to forget to include a purge task. This causes ePolicy Orchestrator to retain every single event since the McAfee ePO server was built. You can fix this simply by creating a purge task. See *Purge events by query* for details.

But, if you notice one or two events make up a disproportionate number of your events then determine what they are by drilling down into those events. For example, in the previous figure you see that the event with the most instances is an access protection rule from VirusScan Enterprise. This is a very common event. If you double-click on the Access Protection rule event to drill down on the cause you can see in the following figure. You find there a few access protection rules that are being triggered repeatedly on VirusScan Enterprise.



GY-All Threat Events by Description -> Access Protection rule violation detected and NOT blocked

Show selected rows

Event Generated Time (UTC)	Threat Target Host Name	Threat Name
12/19/09 1:33:27 AM	JAVATEK1VM	Virtual Machine Protection:Prevent Termination of VMWare Processes
12/24/09 7:12:49 PM	JAVATEK1VM	Common Standard Protection:Prevent common programs from running files from the Temp folder
12/26/09 7:59:50 PM	JAVATEK1VM	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/2/10 6:35:45 PM	JAVATEK1VM	Virtual Machine Protection:Prevent Termination of VMWare Processes
1/14/10 2:17:10 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:11 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:11 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:11 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:12 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:12 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:12 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:12 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:12 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:12 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder
1/14/10 2:17:13 PM	W7MANGHART	Common Standard Protection:Prevent common programs from running files from the Temp folder

10 At this point determine if these are important events in your organization, or if they are even being looked at by administrators. Ignoring some events is very common by some administrators.

Ultimately, whenever dealing with excessive events in your database you must follow this process:

1 Create a query showing all events you are questioning using the information in this section to analyze these threat events.

2 Determine if anyone is looking at these excessive events in the first place

3 If events are not being analyzed, change your policy to stop the event forwarding

4 If the event is important, make sure you are monitoring the number of events using the *Creating event summary queries* and *Purging events automatically* appropriately.

So if you are not looking at these events in the first place then you may consider disabling the event completely in the VirusScan Enterprise access protection policy to stop the event from being sent to the McAfee ePO server in the first place. Alternatively, you can adjust your policy to only send the access protection events you are concerned with instead of excessive events that are not being analyzed. If you do want to see these events then you can leave the policy as configured, but make sure you are following the rules about purging events from the McAfee ePO server to make sure these events do not overrun your database. See *Purging events automatically* for details.

Creating custom table queries

You can create a simple table query to take an action on events. For example, you might need to purge data or events based on a query. Or you might have events of a specific type that are overwhelming your database. For example, see *Filtering 1051 and 1059 events*.

A table query is used to returns data in a simple table format, without graphs or charts. Simple table data can be acted upon by an ePolicy Orchestrator server task. For example, allowing you to automatically delete this data.

Create a custom query that returns all 1051 and 1059 events in the ePolicy Orchestrator database.

Task

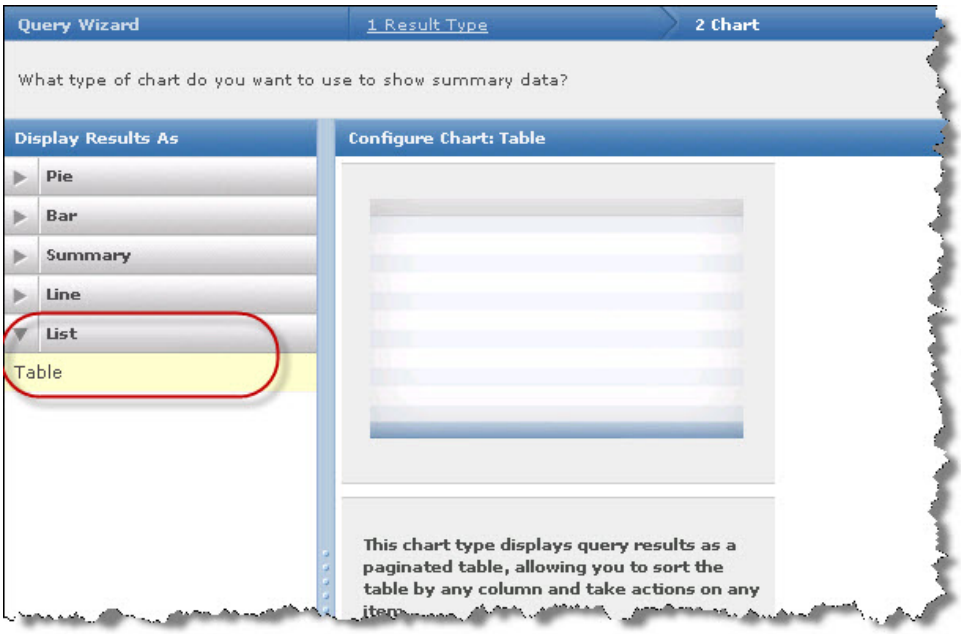
For option definitions, click **?** in the interface.

1 Click **Menu | Reporting | Queries**, the Queries dialog box appears.

2 Click **Actions | New Query** and the Query Wizard appears starting with the Result Types tab.

3 Click **Events** in the Features Group and **Client Events** in the Result Type.

4 Click **Table**, under List, in the Display Results As pane to create a simple table format and click **Next**.


Query Wizard
1 Result Type
2 Chart
What type of chart do you want to use to show summary data?
Display Results As
Configure Chart: Table
Pie
Bar
Summary
Line
List
Table
This chart type displays query results as a paginated table, allowing you to sort the table by any column and take actions on any

5 Click **Next** to skip the Columns dialog box. You can choose the columns you want to analyze.

> You can skip this step because the McAfee ePO server does not use the columns you choose in the server task.

6 Click **Event ID** in Available Properties under Client Events to create an Event ID filter. An Event ID row is added in the Filter pane.

7 Click the plus sign, **+**, at the right to add another comparison row, add `1051` and `1059` in the Value column, then click **Run**.

This setting filters the query and only returns 1051 and 1059 events as shown in the following output figure.

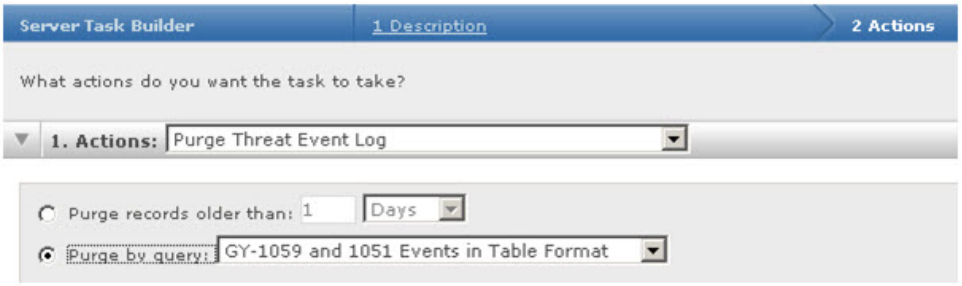
8 Optionally, you can select all of these 1051 and 1059 events, click **Actions | Purge** to purge all of these events in real time.

Instead of purging the events in real time during business hours you can create a server task that runs the purge nightly during off hours. See *Purging events automatically* for details.

9 Create a new server task and give it an appropriate name. For example, `Purge of 1051 and 1059 Events Nightly`.

10 Click **Purge Threat Event Log** from the Actions list, then click **Purge by Query**.

11 Find the custom query you just created and click it in the list.



12 Schedule the task to run every night, then click **Save**.

You can use this technique to purge other threat events based on the custom table queries you create.

12 FAQ and common scenarios

This chapter contains some frequently asked questions (FAQs) and some common scenarios that an ePolicy Orchestrator administrator might have when configuring the McAfee ePO server.

Contents

- *Determining if you have a duplicate GUID problem*
- *Determining if your server has performance problems*
- *Understand product version numbers*
- *Determining the best upgrade strategy*
- *1051 and 1059 events*

Determining if you have a duplicate GUID problem

One of the most common problems you might encounter are McAfee Agents with duplicate GUIDs.

In ePolicy Orchestrator 4.5 and later, you can use a preconfigured server task that runs a query and targets machines that might have duplicate GUIDs. This task tells the agent to regenerate the GUID and fix the problem. See the *McAfee ePolicy Orchestrator 4.5 Product Guide* for details.

In ePolicy Orchestrator version 4.0 and earlier, the only way to solve this problem was to redeploy the agent.

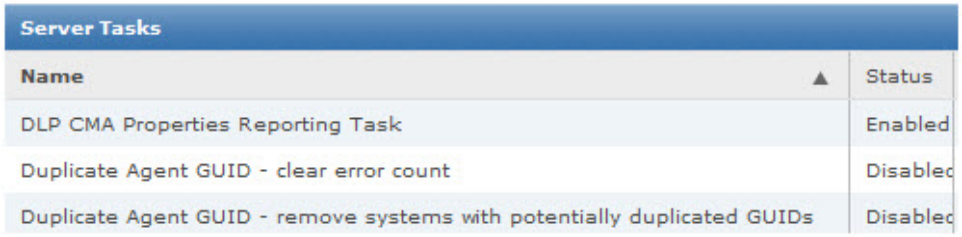
Run the duplicate GUID server task.

Task

1 Click **Menu | Automation | Server Tasks** to open the Server Tasks Builder.

2 Click **Edit** for one of the following tasks.

- **Duplicate Agent GUID** — Clear error count.
- **Duplicate Agent GUID** — Remove systems with potentially duplicated GUIDs.



3 In the Description page, select **Enabled**, then click:

- **Save** — To enable the server task and run it from the Server Task dialog box.
- **Next** — To Schedule the server task to run at a specific time and perform the task.

Determining if your server has performance problems

If you suspect your ePolicy Orchestrator server is having performance problems, check to see how hard your ePolicy Orchestrator server is working. First use Windows Task Manager, then Windows Server 2008 Reliability and Performance Monitor.

Using Windows Task Manager

If your McAfee ePO server is having performance problems, start Windows Task Manager on the server and check:

- ePolicy Orchestrator server performance
- For excessive paging
- Is the physical memory being used
- Is the CPU overutilized

Using Windows Reliability and Performance Monitor

A common feature that is often neglected is the Windows Server 2008 Reliability and Performance Monitor counters for the McAfee ePO server. These counters are added to the Windows Reliability and Performance Monitor when ePolicy Orchestrator is installed. They are extremely informative and can give you an idea of how hard the McAfee ePO server is working.

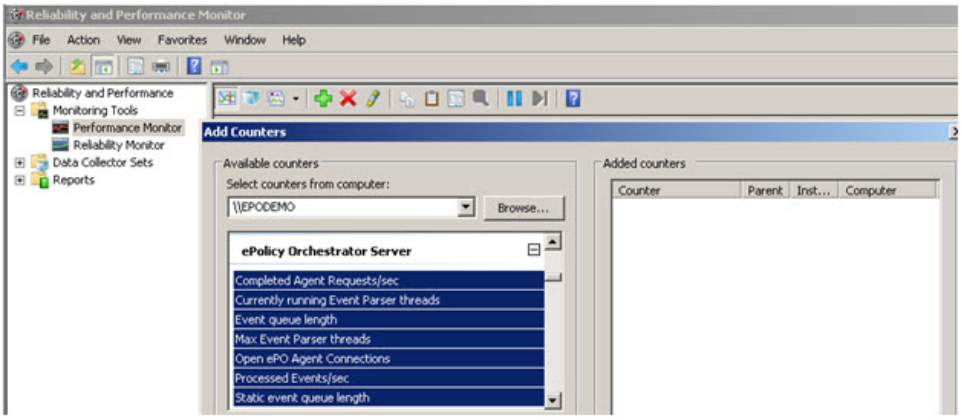
Access these McAfee ePO server counters from the Windows 2008 Server.

Task

1 Under Reliability and Performance, click **Monitoring Tools | Performance Monitoring**, then click the plus sign (**+**). The Add Counters dialog box appears.

2 In the Available counters list, browse to the computer to test, or scroll down to the ePolicy Orchestrator Server counters selection, then click the plus sign (**+**) to expand the list of counters.

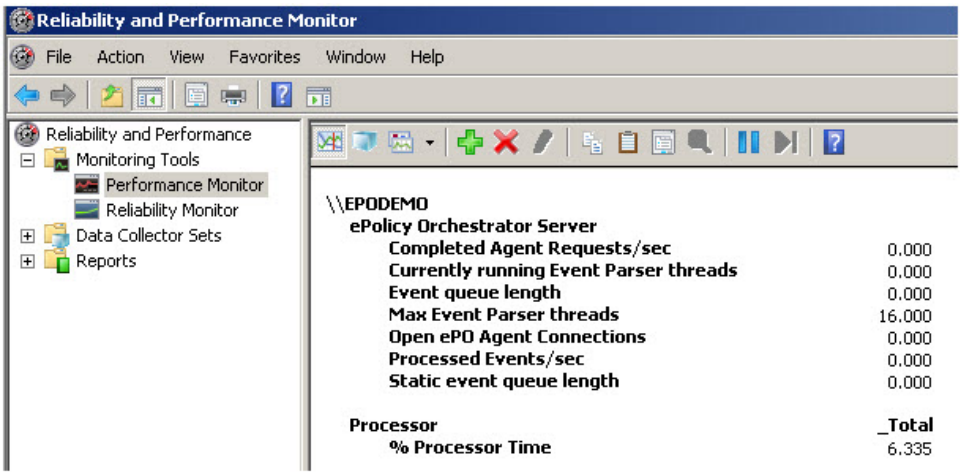
The following figure shows the Windows Reliability and Performance Monitor and the ePolicy Orchestrator Server available counters.



3 Click **Add** to move the selected counter into the Added counters list and click **OK**.

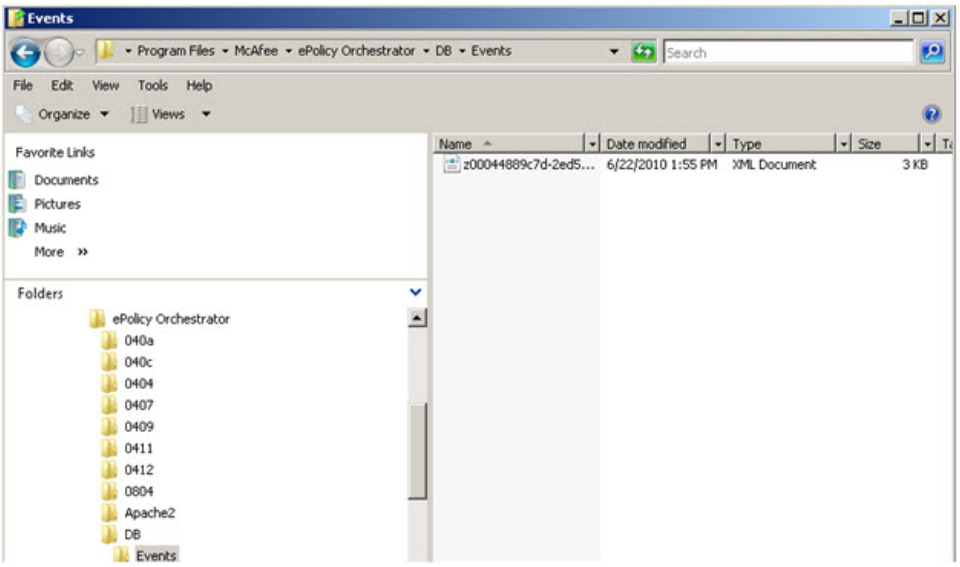
An important number to check is the **Open McAfee Agent Connections**. This counter tells you how many McAfee Agents are communicating with the McAfee ePO server simultaneously. A healthy ePolicy Orchestrator server keeps this number fairly low, usually under 20. An ePolicy Orchestrator server that is struggling shows this number over 200 (the maximum is 250) and it stays at that number and rarely gets under 20.

Another important indicator of the stress on your ePolicy Orchestrator server is how quickly it can process events from all your agents. The following figure is an example.



You can also check how quickly your ePolicy Orchestrator server processes events from agents by looking in the Events folder on the McAfee ePO server. This folder is where all events are processed by ePolicy Orchestrator and sent to the SQL database. You can find this folder at:

```
C:\Program Files\McAfee\ePolicy Orchestrator\DB\Events
```



At any time, this folder might display a few dozen or a few hundred events.

In larger environments this folder is constantly processing thousands of events per minute.

If you click the **Refresh** button and look at the status bar you can see the number of files in this folder changing very quickly. If there are thousands of files in this folder and ePolicy Orchestrator is unable to process them then it is probably struggling to process the events at a reasonable rate. It is normal for this folder to fluctuate depending on the time of day, but if there are thousands of files in this folder and it is constantly increasing then this probably indicates a performance issue.

Understand product version numbers

As with all software products new patches and hotfixes are released on a regular basis to update bugs and add new features. If you are a new McAfee user it might help to understand the McAfee product version numbering system.

Each major product version number is followed by a build number. The build number represents the patch applied to the product. McAfee patches are typically just sequential numbers. For example, release patch 1, patch 2, patch 3, as required. If you look at the McAfee McAfee Agent version 4.0, the actual version number is: 4.0.0.1421

Where:

- "4.0.0" — Is the product revision number
- "1421" — Is the build number. That build number indicates this is "Patch 2"

To determine the build number-to-patch number relationship you must go to the KnowledgeBase (KB) articles for each product. See *Reference documentation*.

ePolicy Orchestrator server and McAfee Agent revisions

The two most relevant products for this document are the McAfee ePO server and the McAfee Agent. Many users assume that the McAfee Agent version number must match the McAfee ePO server version number. This is not true.

The agent and server versions are disjointed and do not have to be on the same major version. For example, the McAfee ePO server 4.5 works fine with McAfee Agent 4.0 or 4.5.

There are limits to how far back the McAfee ePO server supports McAfee Agents and those limits are clearly defined in the McAfee KnowledgeBase articles for the products.

Determining the best upgrade strategy

If you are ready to upgrade you're the McAfee ePO server and your McAfee Agent you probably want to know which product to upgrade first. There is no recommended order, but to approach it logically upgrade the McAfee ePO server software first.

Upgrading your McAfee ePO server software first makes your backend architecture ready to speak to your newly upgraded agents, when that occurs. Also, when you upgrade the McAfee ePO server you are only impacting one device, you're the McAfee ePO server, compared to upgrading the agents which impacts all devices in your environment.

1051 and 1059 events

If you have not looked at your Event Filtering in a long time on your McAfee ePO server, run the custom Event Summary Query and check the output. See *Event summary queries* for details.

The two most common events seen in customer environments are:

- 1051 — Unable to scan password protected file
- 1059 — Scan timed out

These two events are enabled by default on the McAfee ePO server and if you never disabled them you might find a significant number of these events when you run the Event Summary Query. These two events can, for some users, make up 80% of the events in the database, use a tremendous amount of space, and impact the performance of the database.

So why are they in there and why are they enabled? They have historic significance going back several years and they were meant to give the administrator full disclosure that a file was not scanned by VirusScan Enterprise. This failure to scan the file could be for one of two reasons:

- Because the scan timed out due to the size of the file, which is a 1059 event
- The file was not scanned because it was inaccessible due to a password or encryption on the file, which is a 1051 event

Disable these two events under event filtering to prevent a flood of these events into your database. By disabling these events you are effectively telling the agent to stop sending these events to ePolicy Orchestrator.

These events are still logged locally by VirusScan Enterprise in the On-access scanner log file for reference on the local client.

Optionally, you can disable additional events but this is not typically necessary since most of the other events are important and are usually generated in manageable numbers. Plus, you can enable additional events as long as you monitor your event summary query to make sure that the new event you enabled does not overwhelm your database.

Filtering 1051 and 1059 events

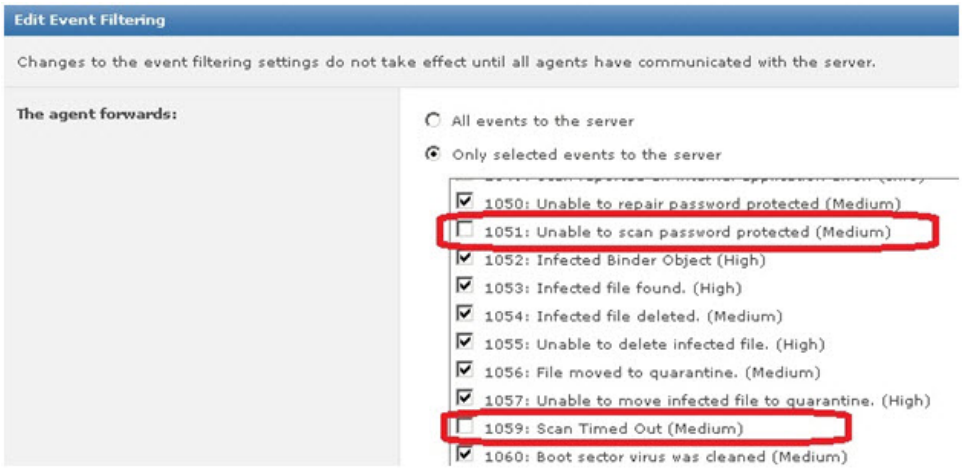
Disable the 1051 and 1059 events if you find a significant number of these events when you run Event Summary Query.

Task

1 Under Setting Categories, click **Menu | Configuration | Server Settings**, **Event Filtering**, then **Edit**. The Edit Event Filtering dialog box appears.

2 From The Agents Forwards list, scroll down until you see the following events, and deselect them:

- 1051: Unable to scan password protected (Medium)
- 1059: Scan Timed Out (Medium)


Edit Event Filtering
Changes to the event filtering settings do not take effect until all agents have communicated with the server.
The agent forwards:
All events to the server
Only selected events to the server
1050: Unable to repair password protected (Medium)
1051: Unable to scan password protected (Medium)
1052: Infected Binder Object (High)
1053: Infected file found. (High)
1054: Infected file deleted. (Medium)
1055: Unable to delete infected file. (High)
1056: File moved to quarantine. (Medium)
1057: Unable to move infected file to quarantine. (High)
1059: Scan Timed Out (Medium)
1060: Boot sector virus was cleaned (Medium)

3 Click **Save**.

13 SQL maintenance

For your McAfee ePO server to function correctly it is very important to have a well performing SQL database. It is the central storage place for all the data your McAfee ePO server uses and it requires maintenance and care.

ePolicy Orchestrator SQL database maintenance

The SQL database used by the McAfee ePO server requires regular maintenance and back ups to ensure ePolicy Orchestrator functions correctly.

On a regular basis, perform these tasks to make sure your SQL Server is maintained:

- Regularly back up of the ePolicy Orchestrator SQL database and its transaction log
- Reindex your database on a regular basis
- Rebuild your database on a regular basis
- Purge older events using server tasks as described in *Purging events automatically*.

The ePolicy Orchestrator SQL database houses everything that ePolicy Orchestrator needs to function. Your System Tree structure, your policies, administrators, client tasks, and configuration settings for the ePolicy Orchestrator server itself. Back up your SQL database regularly in the case your SQL database or your McAfee ePO server environment fails. These backups ensure that if the McAfee ePO sever needs to be rebuilt or restored there is a safe and current copy to revert back to. Plus, if you are using the Microsoft Full Recovery Model for SQL, then your transaction log can continue to grow indefinitely until a full backup is performed.

Table data fragmentation

Probably one of the most significant performance problems found in databases is table data fragmentation. For example, table fragmentation could be similar to an index at the end of a large book. A single index entry in this book might point to several pages scattered throughout the book. This means you must then scan each page for the specific information you are looking for.

This is significantly different from the index of the telephone book that stores its data in sorted order. A typical query for the name "Jones" might span multiple consecutive pages, but are they are always in a sorted order.

In the case of a database, you start out with the data looking like a telephone book and, over time, end up with the data looking more like a large book index.

Therefore, you need to occasionally re-sort the data to recreate the phone book order. This is where re-indexing and rebuilding your ePolicy Orchestrator SQL database is critical. Over time your database becomes more fragmented especially if it manages a larger environment where thousands of events are written to it on a daily basis.

Setting up a maintenance task to automatically reindex and rebuild your ePolicy Orchestrator SQL database only takes a few minutes and is essential to maintain proper performance on the McAfee ePO server. You can include the re-indexing as part of your regular backup schedule to combine everything in one task.

Do **not** shrink your database. This is a common misconception that many administrators choose when building their maintenance task.

To learn the details on creating your maintenance task, see KnowledgeBase article KB67184.

You can learn more about database fragmentation and how to determine the fragmentation of your database, use the DBCC command found in the *Understanding SQL Server's DBCC SHOWCONTIG* article, found at http://www.sql-server-performance.com/articles/dba/dt_dbcc_showcontig_p1.aspx.

14 Disaster recovery

Many ePolicy Orchestrator users want to know how to set up ePolicy Orchestrator for a disaster recovery scenario. There are a few options available depending on your tolerance of risk and budget available for the additional hardware.

Many users think if the McAfee ePO server fails the McAfee Agents on the endpoints and the installed point products stop working properly or malfunction in some way. On the contrary, all agents on your endpoints simply try to contact the McAfee ePO server on their next communication interval and see that the McAfee ePO server is not available. The agents simply try again at a later time. While the McAfee ePO server is unavailable, any events that are generated are sent to ePolicy Orchestrator when it becomes available again and the last policies pulled from ePolicy Orchestrator continue to be used and enforced on the client.

The McAfee ePO server can be unavailable for extended periods of time in a disaster scenario with no impact to your managed machines. The only negative impact is that you are unable to:

- Login to the McAfee ePO server to run reports
- Change polices or tasks since the McAfee ePO server GUI is unavailable
- See any new events reported by the clients

Contents

- *Configuring simple disaster recovery*
- *Use server clusters for disaster recovery*
- *Use cold and hot spares on one physical site*
- *Use cold and hot spares on two physical sites*

Configuring simple disaster recovery

The simplest method of disaster recovery is to rebuild the McAfee ePO server and restore the SQL database that you have backed up for safe keeping. This is a good option if you are a small environment (5,000 to 25,000 nodes) and if you have a reasonable tolerance for downtime.

This means if your server has a hardware failure to get your McAfee ePO server up and running again you must:

Task

1. Repair the McAfee ePO server.
2. Reinstall the ePolicy Orchestrator software.
3. Patch the ePolicy Orchestrator software back to the previous levels.
4. Restore the SQL database.

Full restore procedures are covered in KnowledgeBase article KB66616.

Use server clusters for disaster recovery

If you require zero downtime if a hardware failure occurs you can cluster your ePolicy Orchestrator and SQL servers. But, this requires additional hardware and increases the cost of implementation.

You might chose to only cluster the SQL Servers, which is a more common option, and SQL should have zero downtime. If the McAfee ePO server fails due to hardware failure you can reinstall its operating system, which only takes a few hours, and point the McAfee ePO server to your SQL database. As long as the SQL server is clustered there is minimal value gained if you cluster the McAfee ePO server. McAfee does not recommend clustering the McAfee ePO server because of the increased hardware investment and it increases the complexity of the ePolicy Orchestrator implementation. But it does work.

The full restore procedures are described in the KnowledgeBase article KB66616.

Use cold and hot spares on one physical site

If your large production environment requires minimal downtime you can use a cold or hot spare McAfee ePO server. The spare server is running a clean installation of ePolicy Orchestrator and pointing to your SQL database.

If you only have one physical site, you cluster your SQL server, and then if your McAfee ePO server fails you can simply change the IP address of the spare McAfee ePO server to the IP address of the failed McAfee ePO server. This is completely transparent to all of the agents and provides the least downtime in a disaster situation.

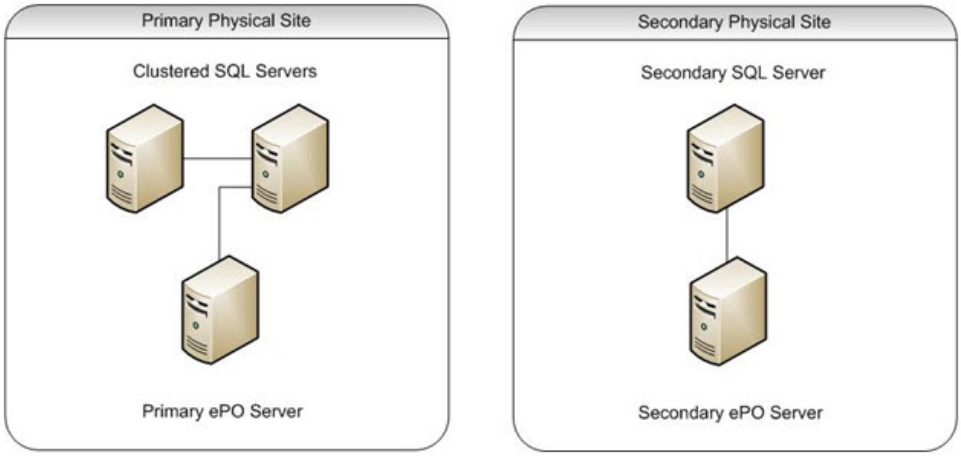
You must have a good SQL database backup for this to work.

The full restore procedures are described in the KnowledgeBase article KB66616.

Use cold and hot spares on two physical sites

If you want total disaster recovery use two physical sites with a primary site and a secondary site.

Your primary site should have a clustered SQL Server and a single McAfee ePO server. The secondary site should have a hot or cold spare McAfee ePO server and an SQL database. You can use SQL replication or SQL Log Shipping to copy the ePolicy Orchestrator database from the primary site to the secondary site's SQL server on a nightly or weekly basis during non business hours. Then you need to make sure your secondary McAfee ePO server is pointing to your secondary SQL server. See the Microsoft article Types of Replication Overview for details.



Now, if the primary site fails you must make all the agents previously communicating with the primary McAfee ePO server start communicating with the secondary McAfee ePO server located at another physical site that has a different IP address and different DNS name. Remember, the agents find the McAfee ePO server by communicating to its IP address first and if that fails they use its DNS name. If the agents see that the primary site's IP address is not available they will query DNS where you will have changed the IP address for the primary McAfee ePO server to point to the IP address of the secondary McAfee ePO server. All agents then instantly start pointing to the secondary McAfee ePO server.

The full restore procedures are described in the KnowledgeBase article KB66616.

15 Reference documentation

Following are several informative and valuable links for your McAfee implementation.

Product videos

Support Video Tutorials— These are video tutorials listed by product and created by the McAfee Support Team

McAfee Corporate YoutTube — Corporate McAfee YouTube Channel with McAfee Messaging

McAfee Technical YouTube — McAfee Technical YouTube Channel focused on Product Videos

McAfee Video Library — A video library describing the value of McAfee Products and includes Technical Tips

Documentation and Support

Product Documentation — Covers all McAfee products and includes product guides, installation guides, and release notes

Knowledge Base Search — The official McAfee KnowledgeBase launching page for McAfee Support Portal. This should be your first resource.

McAfee Community — Public Community for answering questions and discussions with McAfee users

Important McAfee KB Articles

KB59938 — Version Information for the ePolicy Orchestrator server

KB53238 — Version Information for the McAfee Agent 4.0

KB68472 — Version Information for the McAfee Agent 4.5

KB65812 — Master index of release notes for all versions of McAfee products

KB51109 — Every operating system supported by every McAfee product

KB65897 — Master list of support articles for ePolicy Orchestrator 4.5

KB54602 — Troubleshooting ePolicy Orchestrator Notifications and Events

KB67184 — Maintenance plan for SQL with SQL Management Studio

KB66616 — ePolicy Orchestrator 4.5 Server Disaster and Recovery Procedure

KB51670 — Troubleshooting logging into the ePolicy Orchestrator console

KB66797 — Ports required by ePolicy Orchestrator and their functionality

Other Informative Articles

Deploying SQL Server 2005 with SAN #1

Deploying SQL Server 2005 with SAN #2

Deploying SQL Server 2005 with SAN #3

SQL Storage Top 10 Best Practices

Microsoft SQL Technical Documentation

Comparing RAID Implementations for SQL

Is RAID 5 Really a Bargain?

Battle Against Any RAID Five-BAARF

Viewing and Fixing SQL DB Fragmentation

Index

A

about this guide 7
Active Directory
    organizing the System Tree 51
    synchronization 46, 51
AD, See Active Directory
Agent Handlers
    about 11, 35
    increased node count 17
agent-server secure communication
    default interval 40
    exporting keys 40
    about 11
agent-to-server communication interval, about 56
agents
    moving between ePolicy Orchestrator servers 40
    about 43
    adding it to your image file 48
    and SuperAgent repositories 23
    copying the agent file 44
    deleting inactive clients 77
    deploying with third-party tools 47
    functionality 43
    GUID 48
    missing from shell machines 46
    policies 56
    revision numbers 102
    troubleshooting deployment 46
    upgrade strategy 103
Apache server 21
Application Control, about 9
ASCI, See agent-to-server communication interval
ASSC, See agent-server secure communication
automatic responses 11

B

back ups
    database 105, 107
    required with spare database 108
    Secure Sockets Layer certificates 39
    using a SAN 17
    when moving ePolicy Orchestrator server 39
    your infrastructure 37

C

clients
    moving with Transfer Systems 40
    asks, deploying products 63
    converting to SuperAgents 23
    tasks, about 63
configuration
    agent to server communication interval 58
    client event summary queries 88
    custom queries 82, 84
    disabling 1051 and 1059 events 104
    email and export reports from queries 71
    event purging 74
    event purging with a query 76
    Global Updating limitations 32
    hard disks 14
    inactive system deletion 77
    policy enforcement interval 59
    product deployment 64
    queries with tables 95
    server tasks that act on a query 70
    threat event summary queries 91
console, See ePolicy Orchestrator
conventions and icons used in this guide 7
CPUs
    assign priority in virtual machines 14
    needed for node count 29
    overutilized 100
    recommended hardware 17

D

DAT files
    deploying to repositories 27
    updating automatically 72
    using repositories 21
Data Loss Protection, about 9
databases
    64-bit operating systems 17
    about 11
    back up and restore 37, 39
    configuring hard disks 14
    dedicated hard disk 14
    deployed on storage area networks 17

databases *(continued)*
installed with ePolicy Orchestrator 13
maintaining 105
recommended hardware 17
reindex 105
restoring 107
server clusters for disaster recovery 108
sharing hardware with ePolicy Orchestrator 14
spares on physical sites 108
deployment
agents overview and troubleshooting 46
agents with third-party tools 47
calculating repository bandwidth 28
databases on storage area networks 17
packages 60
products 63
to repositories 27
detection definition files, See DAT files
disaster recovery 107
DLP, See Data Loss Protection
DNS
changing ePolicy Orchestrator name 39
used to find the ePolicy Orchestrator server 44, 108
documentation
audience for this guide 7
product-specific, finding 8
typographical conventions and icons 7
drives, See hard disks

E

email and export reports from queries 71
Encrypted USB Drives, about 9
Endpoint Encryption, about 9
ePolicy Orchestrator
moving agents between servers 39, 40
back up your infrastructure 37
components 11
configuring hard disks 14
console 11
dedicated hard disk 14
disable server as repository 29
disaster recovery 107
functions 11
history 9
installed with database 13
installing the software 37
moving agents between servers 39, 40
node count 13
products list 55
recommended hardware 17
repository branches 60
server 11
server clusters for disaster recovery 108
sharing hardware with database 14
spares on physical sites 108
ePolicy Orchestrator *(continued)*
understanding agent version 102
updating the software 37
upgrade strategy 103
events
1051 and 1059 filtering 103
causing ePolicy Orchestrator performance problems 100
creating queries 95
disabling 1051 and 1059 events 104
purge automatically 74
purge with a query 76
purging form database 105
extension, definition 55

F

fragmentation in the database 105
FramePkg.exe, agent installation application 47
FTP repositories 22

G

Global Updating, about 32
groups
in the System Tree 52
of SuperAgents 23
sending a policy change 56
used to deploy products 63
used to store inactive systems 77
GUIDs, deleting from the image file 48

H

hard disks
configuring 14
dedicated 13, 14
recommended hardware 17
hardware
moving ePolicy Orchestrator 39
questions 13
recommend for ePolicy Orchestrator and database 17
recommended configurations 14
sharing with ePolicy Orchestrator and database 14
used for repositories 29
Host Intrusion Prevention, about 9
hotfixes 102
HTTP repositories 22

I

IIS, See Microsoft IIS server
image file, adding the agent 48
installation
ePolicy Orchestrator 37
rebuild ePolicy Orchestrator and database servers 107
IP address
change to move your ePolicy Orchestrator server 39
used to find the ePolicy Orchestrator server 44

IP address *(continued)*
used to sort the System Tree 52

L

LDF file 14

M

master repository
default 29
disabling from ePolicy Orchestrator server 73
on ePolicy Orchestrator 21
McAfee Agents, See agents
McAfee ePolicy Orchestrator, See ePolicy Orchestrator
McAfee ServicePortal, accessing 8
MDF file 14
Microsoft IIS server 21
Microsoft SQL database, See database

N

NAT, See Network Address Translation
Network Address Translation, Agent Handlers 35
node counts
and repositories 23
hard disks 14
questions 13
recommended hardware 17
repository hardware 29
setting agent to server communication interval 56
sharing hardware 14
using virtual machines 14

O

operating systems
64-bit 17
configuring hard disks 14
for repositories 21

P

packages
about 55
deploying 60
patches
reinstall after server restore 107
revision numbers 102
using repositories 21
policies
about 55
creating SuperAgent 23
for agents 56
inherited from System Tree 55
sending immediately 56
policy enforcement
interval 63
policy enforcement *(continued)*
interval configuration 59
products
deployment 63
updating automatically 72
version numbers 102

Q

queries
client event summary 88
creating custom 82, 84
creating reports 81
event summary overview 88
Managed Inactive Agents 77
threat event summary 91
using tables 95

R

RAID 14
RAM
recommended hardware 17
repository servers 29
randomization, product deployment 63
reports
creating 81
creating custom queries 82, 84
email and export output from queries 71
repositories
about 21, 27
branches 60
calculating bandwidth use 27
DAT file replication 28
determine how many and location 27, 29
do not use Agent Handlers 35
FTP servers 22
HTTP servers 22
SuperAgent 23
UNC shares 22

S

SAN, See storage area networks
scheduling
email and export reports from queries 71
event purging 74, 76
product deployment 64
server tasks that act on a query 70
Secure Sockets Layer certificate back ups 39
Security Innovation Alliance 9
server clusters
for disaster recovery 108
for SQL database hardware 14
server tasks
about 69

server tasks *(continued)*
acting on a query 69
servers
combining ePolicy Orchestrator and database 13
disaster recovery 107
finding performance problems 100
platform, questions 13
recommended hardware 17
ServicePortal, finding product documentation 8
shell machines, about 46
SIA, See Security Innovation Alliance
SiteAdvisor, about 9
SQL database, See databases
SQL replication, required with spare database 108
SSL, See Secure Sockets Layer certificates
storage area networks, configuring 17
SuperAgents
configuring 23
sharing hardware 29
synchronization, Active Directory 46
System Tree
configuring SuperAgent group 23
inherited policies 55
organizing with Active Directory 51

T

Technical Support, finding product information 8
ticketing system 11
Transfer Systems, used to move clients 40
troubleshooting agent deployment 46

U

UNC share repositories 22
Universal Naming Convention, See UNC share repositories
updates
DAT files and products automatically 72
ePolicy Orchestrator 37
upgrading product strategy 103

V

virtual machines
configuring hard disks 14
node count 14
testing ePolicy Orchestrator 37
with database 14
with ePolicy Orchestrator 14
VirusScan Enterprise, about 9
VMs, See virtual machines

W

Windows Reliability and Performance Monitor 100
Windows Task Manager 100